

The Dynamics of Data Donation: Privacy Risk, Mobility Data, and the Smart City

Jorge Fernando Pereira Campos



University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of
Doctor of Philosophy (PhD)
at the University of St Andrews

January 2021

Candidate's declaration

I, Jorge Fernando Pereira Campos, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 80,000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

I was admitted as a research student at the University of St Andrews in September 2017.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 26/05/2021

Signature of candidate

Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date 26/05/2021

Signature of supervisor

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Jorge Fernando Pereira Campos, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed copy

No embargo on print copy.

Electronic copy

No embargo on electronic copy.

Date 26/05/2021

Signature of candidate

Date 26/05/2021

Signature of supervisor

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Jorge Fernando Pereira Campos, understand that by declaring that I have original research data or digital outputs, I should make every effort in meeting the University's and research funders' requirements on the deposit and sharing of research data or research digital outputs.

Date 26/05/2021

Signature of candidate

Permission for publication of underpinning research data or digital outputs

We understand that for any original research data or digital outputs which are deposited, we are giving permission for them to be made available for use in accordance with the requirements of the University and research funders, for the time being in force.

We also understand that the title and the description will be published, and that the underpinning research data or digital outputs will be electronically accessible for use in accordance with the license specified at the point of deposit, unless exempt by award of an embargo as requested below.

The following is an agreed request by candidate and supervisor regarding the publication of underpinning research data or digital outputs:

Embargo on all of electronic files for a period of 5 years on the following ground(s):

- Publication would be in breach of law or ethics or data protection

Supporting statement for embargo request

I have no permission from the participants of my study to publish my research data.

Date 26/05/2021

Signature of candidate

Date 26/05/2021

Signature of supervisor

ABSTRACT

With the development of new technologies and their increased applications in the context of a local government, cities have started to claim that they are smart. Smart Cities make use of Information and Communication Technologies (ICTs) to support planning and policy making. For an appropriate and sustainable functioning of these smart cities, collecting data about the different aspects of their territory and operations, including its citizens, is a crucial activity. Currently, there are two main avenues in which smart cities can collect data about their citizens: either through sensors, and cameras strategically placed throughout the city or by asking citizens to voluntarily donate to the local government their personal data (i.e., citizen engagement or ‘e-participation’). Despite the growth and increasing prevalence of the latter practice, little attention has been given to how individuals experience the risks of data donation. Often, studies consider data donation as an aspect of the phenomenon of surveillance, or as a type of data sharing. This study theorises and empirically examines data donation and its risks as a phenomenon which is separate from either surveillance or data sharing.

Focusing on mobility data, this study draws on two established donation and privacy risk frameworks to investigate how the risks of donating personal data to a smart city are experienced and socially constructed. The thematic analysis of ten focus groups conducted showed that, in the context of this empirical examination, privacy-specific risks alone do not constitute constructed risks. Instead, they combine in various ways with perceived donation risks to constitute more nuanced and embedded risk

constructions. Donation risks are seen as potential consequences of privacy risks and combined they constitute the risks of donating data. This thesis underlines the importance of the context under which data donation takes place as well as privacy's value in a free and democratic society.

ACKNOWLEDGEMENTS

General acknowledgements

“Adoramos a perfeição, porque a não podemos ter; repugná-lá-íamos se a tivéssemos. O perfeito é o desumano porque o humano é imperfeito.”

- Fernando Pessoa, Livro do Desassossego

“We worship perfection because we can't have it; if we had it, we would reject it. Perfection is inhuman, because humanity is imperfect.”

- Fernando Pessoa, Book of Disquiet

Dedico este trabalho aos meus pais por todo o amor, carinho e força que sempre me deram. Amo-vos!

The doctoral journey I have just been through has been the most challenging endeavour of my life to date. Not only on a professional but also on a personal domain. It was a lonely journey filled with self-doubt, added by the stresses of living through a pandemic. The impostor syndrome and anxiety were my roommates during these past three years, and, I am sure, they will continue to be for the rest of my life. However, what I managed to understand is that they can be put on a leash. Despite the fact that

they will always be part of my life, now I can see that they are not big scary lions, but instead, two little kittens that can often scratch, bite, hurt, but can be easily tamed. If you are reading this now and you are a doctoral researcher, or a professional, or someone who has a dream but are doubting themselves, I want you to find peace in knowing that it is more common than you may believe. You are not alone. Countless times I felt discouraged by critical feedback, by journal rejections, by postdoctoral applications rejections, by lecturer application rejections, and the list goes on. However, if I have learned that it is not what they say it is what you do with what they say, so can you. Instead of feeling down or defeated, you can build on that feedback and prove them wrong.

I am grateful for this journey, and I would like to thank those who supported me through it. These people helped me see beyond the narrow horizon of my own capabilities and believed in me even when I did not believe in myself. In no special order, I would like to thank my parents for always being there for me, for supporting me in my decision to move abroad, and for welcoming back to where I will always belong. Poli, the most special animal in my life is always there to make me company. The high-pitched barking, although sometimes annoying, always manages to put a smile on my face. I am sorry I have been away for too long, but I know you understand. No matter for how long I am away, when I come home, I am so very happy to find you wiggling your tail, barking and begging for treats. My godparents and cousin for always being there for me during all my life and playing such a cornerstone role throughout my upbringing. They are pillars and role-models for me as if they were my second parents. To my grandparents, especially my grandfather Édgar, that

unfortunately are not here anymore, I am sure you all are somewhere looking down on me and guiding me through the difficult times. I am also sure that you are proud of what I have achieved. To my fiancée, Justė for being more than understanding and supportive throughout this journey. It has been challenging and strenuous, and distance surely does not help, but despite all this you still managed to be there to listen to my worries at any time of the day. Also, her parents for always welcoming me to their home. They took care of me as if they were my parents, and I will always cherish the moments we spend together. A huge thank you to Virgilijus Tarutis and Daina Tarutienė. Pipa, the grumpiest dog I have ever met also deserves to be acknowledged. When I was writing in Vilnius, she would always sit next to me looking at the computer almost as if checking if I was writing everything correctly. Often, she would decide when I should take a break and gently nudge my hand off the keyboard and on to her head. No matter how many times you bit me, I will forever love you little Pipoca.

Obviously, a huge thank you to Kirstie for being the best supervisor I could ever wish for, on many different levels. First, your knowledge input and academic advice was always timely, supportive, and critically constructive. Second, for your availability in giving me quick feedback and, often, for being available to meet almost immediately when I was struggling with something. Third, for your personal advice, for listening to and understanding my worries and anxieties. Your support and mentorship have been vital for my development not only as a scholar but also as an individual. My future PhD students will be lucky that I carry all your advice and words of wisdom. Also Sally Dibb, the School of Management, my doctoral colleagues and the rest of

academic staff have been such an inspiration in upholding the University's motto "Ever to Excel".

A huge thank you to Dr Luís Santos who, sadly, I got to see on a regular basis only during my last year of PhD. Thank you for all the advice, and for helping me navigate through the mess that was my brain. I have made a good friend.

To all my friends and family (Daniel, Diogo, and the list is too big to mention), a huge thank you for being part of my life. This would not be possible without your love and support. Raúl, thank you for being as annoying as you are. Life would be less fun if we haven't met – You will always be like a brother to me. Sunny Jain, although you arrived a bit later into my life than the other folks acknowledged, you had a big impact. You helped me find a passion and the patience I didn't know I quite had. I will forever be thankful for a great friend I have made.

Lastly, a huge thank you to everyone who has ever doubted me, or rejected my work, I managed to build on your doubt and criticism to achieve something that years ago was merely a dream. I could not imagine any scenario where I could get through a PhD without any of these people in my life. You are the cornerstone of what I am today, and I will always hold you dearly in my heart and be forever thankful for your continuous support.

One last thing I would like to say to whoever is reading this. Throughout my life I have carried with me two things my grandfather Édgar used to say: "Men don't cry" and "When someone asks you if you know how to do something just say you do, and then

figure it out how to do it later”. Although I understand that, perhaps, the first is not so much about the literal act of crying, but more about not showing that, sometimes, you are vulnerable. I now understand that it is ok to be vulnerable. It is ok to show you are vulnerable, especially to the ones who care about you and your wellbeing: ‘it is ok not to be ok’. Also, it is ok to admit you do not know how to do something and ask for help. You will eventually learn and grow.

Just before delivering my final version of this thesis – I would like to thank Dr Fergus Neville and Professor Priscilla Regan for the insightful Viva discussion and examination.

Funding

This work was supported by the University of St Andrews and the Social Sciences and Humanities Research Council of Canada (SSHRC) under the ‘Big Data Surveillance’ partnership grant. The grant’s reference is: SSHRC 895-2015-1003

Table of Contents

ABSTRACT.....	5
ACKNOWLEDGEMENTS	7
CHAPTER 1: INTRODUCTION	18
1.1 BACKGROUND.....	19
1.2 SURVEILLANCE	20
1.3 SMART CITIES	25
1.4 CONTRIBUTION OF THE RESEARCH.....	28
1.5 INTRODUCING THE RESEARCHER	31
1.6 THESIS OVERVIEW	34
CHAPTER 2: THE DYNAMICS OF DONATION	37
2.1 INTRODUCTION	37
2.2 TYPES OF DONATION.....	39
2.2.1 Monetary Donation	40
2.2.2 Blood Donation	42
2.2.3 Organ Donation	43
2.2.4 Product Donation.....	44
2.2.5 Time Donation (Volunteering).....	46
2.2.6 Medical Data Donation	48
2.2.7 Data and The Traditional Types of Donation.....	51
2.3 DEFINING DATA DONATION	58
2.4 MOTIVATIONS TO DONATE.....	61
2.4.1 Intrinsic Motivations	62
2.4.2 Extrinsic Motivations	70
2.4.3 Conspicuous Compassion	75
2.5 THE FOCUS ON RISKS	79
2.6 CONCLUSION.....	87
CHAPTER 3: EXPLORING PRIVACY.....	89
3.1 INTRODUCTION	89

3.2 FUNDAMENTALS OF PRIVACY	91
3.2.1 <i>Westin's Approach</i>	92
3.2.2 <i>Clarke's Approach</i>	98
3.2.3 <i>Altman and the Privacy Regulation Theory</i>	104
3.3 PRIVACY AS A SOCIAL VALUE	108
3.3.1 <i>Communication Privacy Management and the Focus on Relationships</i>	108
3.3.2 <i>Privacy at the epicentre of individuation and relationship making</i>	111
3.4 CONTEXTUAL INTEGRITY	115
3.5 PRIVACY-SPECIFIC RISKS	121
3.5.1 <i>A Taxonomy of Privacy Harms</i>	122
3.6 CONCLUSION	127
CHAPTER 4: RESEARCH METHODS AND DESIGN	129
4.1 INTRODUCTION	129
4.2 PHILOSOPHICAL CONSIDERATIONS	131
4.2.1 <i>Ontological Considerations</i>	131
4.2.2 <i>Epistemological Considerations</i>	135
4.3 DATA COLLECTION METHODOLOGY	138
4.3.1 <i>Key Informant Interviews</i>	141
4.3.2 <i>Milton Keynes</i>	143
4.3.3 <i>Focus Groups</i>	146
4.3.4 <i>Vignettes</i>	150
4.4 METHODS DESIGN	154
4.4.1 <i>Sampling and Access Strategy</i>	154
4.4.2 <i>Producing the Vignettes</i>	158
4.4.3 <i>Focus Groups Design</i>	163
4.5 DATA ANALYSIS METHODOLOGY AND METHODS	168
4.5.1 <i>Thematic Analysis</i>	169
4.5.2 <i>Doing Thematic Analysis</i>	174
4.6 ETHICAL CONSIDERATIONS	175
4.7 CONCLUSION	180
CHAPTER 5: RESULTS CHAPTER	181
5.1 INTRODUCTION	181
5.2 INTRODUCTORY QUESTIONS	184
5.3 THE DYNAMICS WITHIN THE FOCUS GROUPS	184

5.4 CONCERNS WITH DATA DONATION: IDENTIFYING AND REINFORCING THE RISKS	187
5.4.1 Data Collection Risks.....	188
5.4.2 Data Processing.....	190
5.4.3 Data Dissemination.....	193
5.4.4 Invasion.....	195
5.4.5 Physical Safety.....	197
5.4.6 Financial.....	199
5.4.7 Psychological.....	201
5.4.8 Time.....	204
5.4.9 Social.....	206
5.4.10 Performance.....	208
5.5 ARGUMENTS FOR DONATION: MITIGATING THE RISKS?	210
5.5.1 Avoidance of Physical Dangers	211
5.5.2 Financial Benefits	214
5.5.3 Psychological Mitigation	217
5.5.4 Improving Life / Saving Time.....	222
5.5.5 Social.....	225
5.5.6 Performance.....	227
5.6 CONCLUSION.....	230
CHAPTER 6: MAKING SENSE OF THE CONSTRUCTION OF RISK	231
6.1 INTRODUCTION	231
6.2 MAKING SENSE OF THE CONSTRUCTION OF RISK.....	233
6.2.1 Traditional Risks → Privacy Risks	233
6.2.2 Intensification of Data Collection Risks	236
6.2.3 Intensification of Risks Related to Data Processing.....	242
6.2.4 Intensification of Data Dissemination Risks.....	245
6.2.5 Intensification of Invasion Risks	252
6.3 MAKING SENSE OF THE MITIGATION OF CONSTRUCTED RISK.....	254
6.3.1 Traditional Mitigatory Arguments → Privacy Risks	255
6.3.2 Mitigation of the Constructed Data Collection Risks	256
6.3.3 Mitigation of the Constructed Data Processing Risks	263
6.3.4 Mitigation of the Constructed Data Dissemination Risks.....	265
6.3.5 Mitigation of the Constructed Invasion Risks	267
6.3.6 Traditional Mitigatory Arguments → Traditional Risks	269
6.4 CONCLUSION AND FINDINGS	271

CHAPTER 7: DISCUSSION	278
7.1 INTRODUCTION	278
7.2 EMPIRICAL CONTRIBUTION	279
7.3 THEORETICAL CONTRIBUTION	283
7.3.1 <i>Data and Donation</i>	283
7.3.2 <i>Privacy</i>	286
7.4 OTHER OBSERVATIONS.....	297
7.4.1 <i>Boundary Negotiations and Relationship Developments in Data Donation</i>	297
7.5 RESEARCH LIMITATIONS	300
7.6 FUTURE RESEARCH DIRECTIONS	303
7.7 POLICY IMPLICATIONS.....	307
7.8 CONCLUDING REMARKS	312
REFERENCES	314
APPENDICES.....	334
APPENDIX 1 – KEY INFORMANT INTERVIEWS QUESTIONNAIRE	334
APPENDIX 2 – FOCUS GROUPS RECRUITMENT QUESTIONNAIRE	336
APPENDIX 3 - VIGNETTES	346
APPENDIX 4 – CODING TREE	348
APPENDIX 5 – ETHICS AUTHORISATION	349
APPENDIX 6 – ETHICS APPLICATION FORM.....	350
APPENDIX 7 – CONSENT FORM.....	365
APPENDIX 8 – PARTICIPANT INFORMATION SHEET	367
APPENDIX 9 – DEBRIEFING SHEET	370
APPENDIX 10 – ETHICAL AMENDMENT FORM	372

List of Tables

TABLE 1 - COMPARISON BETWEEN DATA AND TRADITIONALLY DONATED ASSETS	56
TABLE 2 - CATEGORICAL APPROACHES TO CONCEPTUALISE PRIVACY	103
TABLE 3 - NISSENBAUM’S DECISION HEURISTIC TABLE	118
TABLE 4 - FOCUS GROUPS STATISTICS	183
TABLE 5 - SUMMARY OF NODES CODED AND THEIR FREQUENCY	188
TABLE 6 - SUMMARY OF NODES CODED AND THEIR FREQUENCY	210
TABLE 7 - RISK INTENSIFICATION DYNAMIC.....	236
TABLE 8 – THE DYNAMIC OF THE MITIGATION OF CONSTRUCTED RISKS	255

List of Figures

FIGURE 1 - MOTIONMAP APP, MILTON KEYNES SMART CITY PROJECT (MK: SMART)	26
FIGURE 2 - DYNAMICS OF MEDICAL DATA DONATION	50
FIGURE 3 - FACTORS INFLUENCING PURE ALTRUISTIC ACTIONS.....	67
FIGURE 4 - INTRINSIC MOTIVATIONS OF DONATION BEHAVIOUR.....	70
FIGURE 5 - MOTIVATIONS TO DONATE	78
FIGURE 6 - RISKS OF DONATION	86
FIGURE 7 - THE REDWAYS NETWORK	145
FIGURE 8 - RISK INTERPLAY	273
FIGURE 9 - DATA COLLECTION RISKS INTERPLAY	274
FIGURE 10 - DATA PROCESSING RISKS INTERPLAY.....	275
FIGURE 11 - DATA DISSEMINATION RISK INTERPLAY	276
FIGURE 12 - INVASION RISK INTERPLAY	277

Chapter 1: INTRODUCTION

Data donation refers to the act, active or passive, by the data donor of transferring their personal information to an entity that is requesting it with the goal of a wider social benefit. Everyday data donation is a novel phenomenon in the wider field of donation studies and in studies of privacy and surveillance. Thus far, data donation research and practice have focused on the donation of medical data, or the donation of personal data in extreme cases, such as the donation of a suicide victim's social media data. This thesis focuses on the donation of data in more everyday settings, rather than the extreme settings previously described.

With the increasingly ubiquitous prevalence of information technologies in people's lives, and, with it, the amount of data generated, and collected by many different institutions, data has been used for a plethora of things, one of which is to aid the planning of cities and their resources. These data can be collected via sensors placed on public roads, traffic lights, amongst other things, but can also be donated by the citizens who wish to participate in their smart city project. The process of capitalising on the development of ICTs by citizens as an opportunity to participate in their city's policy making, and design of services is referred to as 'e-participation'. Data donation to a smart city, mediated by new technologies, can be considered a type of e-participation.

How citizens experience and construct the risks of donating their everyday personal data to their local government is yet to be explored in academia. Often these e-

participation programmes are referred to as surveillance and data sharing and studied as such by academics. Data donation is often subsumed under the heading of either surveillance or data sharing (e.g., He et al., 2017). However, as argued in section 2.3, data donation and data sharing have different characteristics and, therefore, questions arise as to whether they are experienced differently. This research addresses this gap in knowledge and aims to contribute to the understanding of how the risks of donating personal data to a smart city are constructed. It establishes that data donation is a separate phenomenon from data sharing and surveillance. This discussion begins in the next section.

1.1 BACKGROUND

A report by the International Data Corporation (Reinsel, Gantz, and Rydning, 2018) forecasts the amount of existing data to grow from 33 zettabytes, in 2018, to 175 zettabytes by 2025. In fact, over the past decade the data accumulated “far exceeds the data that was available to mankind during the preceding century” (Moorthy et al., 2015, pp. 74). This amount of information is used to, amongst other things, derive insights about individuals, to then target them with products, services, policies, and influence what they do. The big data economy is an ecosystem where data is collected and exchanged through a variety of actors. For example, search engines collect personal data which is then sold to companies that want to advertise their products or services to a specific target audience (Chiru, 2016). In 2013, Cukier and Mayer-Schoenbager introduced the concept of datafication: the phenomenon of turning

everyday activities into data which is then translated into some form of value. For instance, through the use of smart watches, an individual can turn their fitness routine into an array of meaningful data. Data pertaining to the number of steps taken, distance ran, calories burned, heart rate are then translated into insights about the individual's fitness levels and fed back to them. All this amount of data available to any entity brings the issue of surveillance to the fore. What exactly is surveillance?

1.2 SURVEILLANCE

Imagine you are a 15-year-old girl with strict parents. You have been feeling a little sick, nauseous and you notice your period is late. There is a slight chance you are pregnant, so, afraid to even discuss this with your parents and get a doctor's appointment, you run to your local supermarket chain to buy a pregnancy test. Your biggest fear is now confirmed – you are pregnant. You do not know what to do, you do not even know how to tell the big news to your parents. You are afraid, you start thinking whether they will throw you out of home, whether they will not accept the baby, your boyfriend, whether money will be enough, whether you should get a job, one million other things go through your mind. You turn to the internet. You go to forums, you search other people's experiences, you search your supermarket's website for the prices of diapers, blankets, baby clothes. All you want is to have a better idea of what is around the corner. Some time has passed, and you still haven't told your parents. One evening, you arrive home from the school and find your dad very upset on the phone, while your mom is trying to calm him down. "What might have

happened?” – you think to yourself. Your dad is calling the supermarket’s customer service as they just have received, in the mail, discount coupons, on your name, for baby-related products. You can see your dad almost as if screaming at the customer service assistant: “My daughter is only 15! Do you want her pregnant? Are you trying to make her pregnant? She is too young! Why are you sending her this?”. The time you most dreaded has arrived. You have to explain to your parents that it was not the supermarket’s mistake: you are pregnant.

So how did the supermarket find out that the teenage girl was pregnant even before her own parents did? By collecting all the data pertaining to the girl’s interactions with the store: from purchasing a pregnancy test, to researching the prices of baby products, to any other internet and social media interactions the girl may have performed. All this data was collected, processed and insights generated. Based on all the data collected, and then processed and compared with the data from other individuals, the supermarket predicts with a high degree of accuracy whether the pregnancy test was positive, the gender of the baby, and even when the baby is due.

This story, based on real events reported in the New York Time’s article “How do companies learn your secrets”¹, illustrates the ubiquitous presence and impact of surveillance in our society. What exactly is surveillance? How can we define it? Lyon (2008, pp. 2) argues that “where we find purposeful, routine, systematic, and focused attention paid to personal details, for the sake of control, entitlement, management,

¹ <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

influence or protection, we are looking at surveillance”. Purposeful in that surveillance can be justified in relation to a “publicly agreed goal”. Routine as “it happens as we all go about our daily business”. Systematic as it is devised and executed according to a specific schedule. Lastly, focused as it concentrates on personal details. Lyon (ibid) claims that “while some surveillance depends on aggregate data, much refers to identifiable persons, whose data are collected, stored, transmitted, retrieved, compared, mined and traded”.

When considering the wealth of data that is currently generated by every individual in the course of their daily lives, surveillance is no longer solely in the government’s domain, as often thought of, but, instead, is now in the realm of private organisations, and even private citizens². Due to the importance data currently holds to the strategic planning of companies, personal data is often being collected, used, sold by companies without the permission of the data subject³.

The data that is collected can be of different types: “CCTV Images, biometrics such as fingerprints or iris scans, communication records or the actual content of calls, or most commonly, numerical or categorical data” (Lyon, 2008, pp. 3). Data such as the individual’s online behaviour, political inclination, sexual orientation, gender identity, heart rate, location, mobility patterns, income, wealth, stage of life, amongst a plethora of other things can also be collected by companies to serve their own interests. This

² The concept of Lateral Surveillance (see Andrejevic, 2004)

³ According to the Chapter 5 of the GDPR, Data Subject is the end user to whom the data collected belongs to.

data is often used by organisations, as depicted in the example at the start of this section, to, amongst other things, learn about their consumers and target market (source), and predict their future behaviour, thus allowing for more efficient marketing and strategic efforts. The person in the above example had not donated their data. It had been collected about them so that they could be targeted and influenced to purchase products that were of interest.

Surveillance can happen in different contexts. Work surveillance for example, as Ball (2010, pp. 89) suggests that “employee monitoring is nothing new. Clocking in, counting and weighing output and payment by piece-rate are all older forms of workplace surveillance”. In fact, when looking back at classical management perspectives, such as bureaucratic (Weber, 1947), scientific (Taylor, 1911), and administrative (Fayol, 1916) approaches, hierarchy, and control are seen as essential to increase efficiency. Nowadays, organisations capitalise on new technology developments to surveil their employees. Fingerprinting, retina and iris scan, drug and alcohol testing, monitoring of browsing, e-mail and telephone contents, mystery shoppers, health assessments, amongst a variety of other things. All of these serve to inform the firm of their employee’s performance, behaviours, and personal characteristics (Ball, 2010).

A practical example of workplace surveillance is Price Waterhouse Cooper’s (PwC) software ‘Check-in’⁴. This software is not only used within PwC but also

⁴ <https://www.pwc.com/us/en/products/check-in.html>

commercialised to other organisations looking to implement an employee monitoring system. ‘Check-in’ combines location and productivity tracking so that employers know where their workers are at any given moment, and whether they have been in proximity with another person displaying COVID-19 symptoms. Furthermore, the app also allows managers to contact employees whose productivity may have declined. This system has the ability to monitor workers’ location (in or outside the workplace premises), health, and productivity (Rodriguez and Windwehr, 2020).

Surveillance, besides being present in organisations to monitor employees and consumers, is equally present at a local government level. Even moving past the classic focus on CCTV footage, a wealth of different technologies and data are currently being used by cities to, allegedly, improve their road networks, traffic lights, public transportation system, amongst other things. Cities making use of smart technologies, and the Internet of Things, are referred to as Smart Cities. The use of these technologies as an answer to urban issues is a form of urban surveillance. “Although some privacy advocates still believe that privacy-by-design (PbD) and other such built-in solutions could prevent smart cities from becoming surveillance cities, because this relies on the gathering and processing of as much data as possible for the purposes of urban management, the smart city is, at its very foundation, a system of surveillance” (Murakami Wood and Mackinnon, 2019, pp. 176). Whilst it may be true that smart cities have surveillant features, they also have features which make them suitable contexts for studying data donation. Moreover, it is an appropriate context for establishing why data donation is a separate concept from surveillance and data

sharing that warrants sustained empirical attention. The section below explores the concept of smart city.

1.3 SMART CITIES

Citizens are now being called on to engage with their cities more than ever before (Cardullo and Kitchin, 2019). For example, citizens have long been asked to separate rubbish for recycling (Folz, 1991), sign petitions to drive change in their city, engage with participatory budgets, amongst other things, all of which amount to a degree of citizen participation. However, with the constant development of information and communication technologies (ICTs), many other ways of proactively participating and engaging with a city emerged. This is the premise upon which Webster and Leleux (2018) assert the concept of ‘technologically-mediated municipal reciprocity’. The authors hold that ICTs create new avenues for increasing interaction between cities and their citizens. In fact, these technologies, that are even the foundation of many smart cities, not only facilitate public engagement, but also enhance the collection of data, vital for the functions of a smart government, such as city planning.

There is a substantial opportunity for citizens to engage with their local government, and, conversely, the cities to interact with their citizens, mediated by new technologies. These new avenues of interaction between cities and their citizens open the door for the concept of data donation as a form of citizen participation as they move beyond thinking of smart cities as surveillant bodies. For instance, Future City Glasgow,

Glasgow City Council's smart city initiative, launched the MyGlasgow App which, amongst other things, allows citizens to report issues with the public road system. Furthermore, the app also "collects data from citizens on their preferences and their journeys through the city, their transactions and data they produce per household..." (OpenGlasgow Report, 2019, pp. 15). This initiative, widely replicated in other smart city projects, as is the case of Milton Keynes, facilitates the donation and flow of data from an individual to the city council. This way, instead of citizens unwillingly and unknowingly having their data collected by sensors and other technologies scattered around their city and fed into their local government, they can choose whether, what, how much, and when to give their data to them.



Figure 1 - MotionMap App, Milton Keynes Smart City Project (MK: SMART)

Source: mksmart.org

Donated data can be of many different types. For example, as illustrated in figure 1, everyday data, such as mobility data, can be donated for the local government to understand how people commute to work, how long they spend in traffic, amongst other things. It can also be used to provide real-time travel information for residents (e.g., how busy and how late is the bus, how busy shops are, amongst other things)⁵.

The donation of everyday data may bring a series of benefits for all stakeholders involved (e.g., data to support policymaking, information on whether a certain bus is late), however, in order for this interaction to function, citizens have to be willing to give their data to the smart city. Accordingly, a tension between donating personal data, contributing to the local government's planning, and support the development of the city, and protecting one's personal information, and privacy emerges.

Furthermore, everyday data donation, as the donation of data generated by an individual's daily routine, is a novel, understudied subject that needs to be investigated. In fact, a quick search on Scopus database using the keywords "data donation" included in the title, abstract, and keywords of papers produced 29 results – about 55% refers to data donation in the health domain, 14% to data donation for research purposes and the rest for different other issues not related to everyday or smart city contexts. There is a clear gap for exploring the construction of risk of data donation in a smart city. This research aims to address this gap and is the first to conceptualise

⁵ <http://www.mksmart.org/transport/>

and define data donation. Specifically, what is the interplay between privacy-specific risks, and other risks present in traditional donation.

1.4 CONTRIBUTION OF THE RESEARCH

The present study develops the concept of everyday data donation and empirically explores how individuals construct the risk of donating their personal data to a smart city. The data was collected through ten focus groups with individuals, aged 35 to 49 who cycled at least once a week for commuting or pleasure purposes. Vignettes were designed to stimulate the discussion around the topic of data donation and to encourage debate around different risks. This way argumentative patterns could be observed and analysed. Furthermore, as it may be a delicate subject for some, the participants were asked to discuss a fictional character, Kris. It was found that individuals initially construct the risk of donating their personal data by identifying privacy specific risks. However, these initially identified privacy risks are then intensified or mitigated by arguments related to the potential consequences that donating data may carry. Accordingly, the contribution of this thesis is that the privacy harms associated with data donation are not constructed as stand-alone harms, by the participants. They are constructed as a precursor to the harmful consequences associated with that donation. Adding to this interplay, it was also found that only certain categories of arguments intensify or mitigate certain identified privacy risk categories.

This research also contributes to privacy and donation broadly. First, it was found that there is a privacy dimension that needs to be considered in the study of data donation, and donation more broadly as this is often a latent topic in the donation literature. Second, support was offered to the concept of privacy as a social value. Participants were receptive to the idea of data donation. For instance, the participants' argumentative patterns vary according to the different social role played in a scenario (e.g., individual as a banker vs as a parent vs romantic partner). Third, contextual elements were observed in the argumentative patterns of the participants offering support to the Theory of Privacy as Contextual Integrity. The concern for the way their personal information flows was evident in the participants' argumentation. For instance, individuals construct risks differently depending on the data processing stage. Lastly, it was found that participants often attempt to negotiate the boundaries and selectively manage the access of others to their personal information. For instance, there was an observable need to separate government, and the non-profit use of one's personal data, from profit-seeking enterprises. This study has contributed to knowledge in these two domains (donation and privacy) by not only providing support and contributing to different theories and shortcomings, in the case of donation research, but also by clearly positioning data donation as a separate concept warranting investigation. It is the first study to define and theorise the emerging phenomenon of data donation as a separate concept, differentiating it from data sharing and from any other type of donation.

In essence, the contribution of this thesis can be summarised by addressing Watson's (1994, pp. S80) "what, why and how framework". This framework helps the researcher

shape their project and better reflect on its design. First, I will address the ‘what?’ of this thesis. This research aims, in simple terms, to explore how individuals perceive the risk of donating their personal data. Data donation refers to the act of giving personal information to an institution which requests it with the objective of promoting public good or for a wider social benefit. The individual willingly gives personal information and is expecting that this personal information, similar to other forms of donation, will somehow have a positive impact in society.

Second, the ‘why?’. As Watson (1994, pp. S80) puts it “why will this be of enough interest to others to be published as a thesis, book, paper, guide to practitioners or policy makers? Can the research be justified as a ‘contribution to knowledge’?”. This thesis, as argued in the first section, addresses an emergent topic that is the use of data generated by the daily routine of an individual for a wider social benefit (i.e. the donation of data). This particular subject has yet to be conceptualised. Moreover, an understanding of how the risks specific to donation interplay with the risks specific to privacy – a dimension added by the fact that the asset donated is an individual’s personal data – has not been explored. What role does privacy actually play in the wider domain of data donation? This research addresses a clear literature gap and ends up contributing to donation and privacy scholarships.

Lastly, ‘how (conceptually)?’ and ‘how (practically)?’. This research builds on two distinct risk frameworks: a donation risk framework proposed by Barkworth and colleagues (2002) – adapted from Mitchel’s (1999) consumer risk framework – and a privacy-specific framework by Solove (2006). These frameworks will work as a priori

frames of reference for the exploration of the two dimensions of data donation (donation and privacy dimensions), as well as in understanding how they interplay in individuals' constructions of risk. Lastly, to address the practical side of the 'how?', this research adopts a social constructionist approach to the study of risk constructions. This thesis recognises that the construction of risk is subjective to individuals and their experiences and cannot be thought of as a reality beyond what is constructed by people through social interactions. Accordingly, focus groups were employed to explore perceptions of risk in the participants argumentative patterns when discussing a series of carefully designed vignettes.

1.5 INTRODUCING THE RESEARCHER

After discussing the background and contribution of this research, I will now introduce myself as the doctoral researcher responsible for producing the first account of everyday data donation, conceptualise it, develop a risk perception framework specific to data donation, and empirically examine it in the context of a smart city. In this brief introduction I will discuss my upbringing and how I went from an industry-focused education to being interested in achieving a doctoral degree in the scholarly world of privacy and surveillance. Hopefully, this introduction will help the reader understand my profile, a little bit of my personality and motivations behind pursuing the highest level of academic qualifications.

I was born in Porto, on the sunny north west coast of Portugal, in the early 90s to a family where pretty much no one has ever gone to higher education, let alone higher education outside of the cosy confinements of Porto. Despite this, achieving an undergraduate degree was never enough for me and I always wanted more. My goal was to reach the highest level of formal education. Accordingly, after finishing my Master's degree, and after successfully achieving a distinction level grade on my dissertation progressing onto a PhD was naturally on my plan. The question, for me, was not if I should apply for a doctoral researcher position, but what should I investigate? To answer this, you should first know about my professional path. Despite the fact that at the time of starting my PhD I was only 25, I had been working since I was 17. Besides the typical teenager summer jobs (waiting tables and driving tourists around Porto in tuk-tuks) I started working as a Marketing executive early on in my studies. This extracurricular work did not only allow me to afford my studies but also gave me invaluable professional experience. After several years working as a full-stack marketer, doing a little bit of everything (social media, performance, analytics, copywriting, SEO) I decided to specialise in the area I loved the most: Analytics. This led me to a Master's degree in Consumer Analytics and Marketing Strategy at the University of Leeds, in the United Kingdom. My interest was not only doing the job of a data analyst, in other words, capturing metadata and other types of data and transforming it into meaningful information. Instead, I wanted to transform the analysed data into actionable insights for the company while contributing for its strategic decisions, and that is where my Marketing and strategic experience came to play. During my Master's and after several consulting tasks I began to critically assess what I was doing and reached the conclusion that some of the work was far from

ethical. Even when some of it was apparently ok, I often questioned what the individual, to whom the metadata I was analysing belongs to, would think about the work I was doing. This is when my interest in privacy and surveillance spurred, and thus started applying for suitable PhD opportunities.

At the end of my Master's degree I was approached by a company with an offer to use my knowledge and experience to perform political profiling and research. The company's name was SCL Elections, the parent company of the now infamous, Cambridge Analytica. At the same time, I had an offer from Professor Kirstie Ball for a PhD at the University of St Andrews. I would be lying if I said the decision was easy. It was not. On one side I had a great job opportunity in London with a massive salary attached. On the other side I had the chance to pursue a dream of mine while working under the supervision of one of the biggest names in Privacy and Surveillance scholarship. Gladly I made the right decision in pursuing my doctoral research. Although very often I doubt(ed) whether I have what it takes to be a researcher, whether Kirstie would have been better off if she chose any other candidate instead of me, and whether I will ever make a name for myself as a researcher, especially when the job market looks this grim, if I was sent back to 2017, I would have made the same decision. The reality is, through the hardship and the many challenges I faced throughout my PhD, I have grown to be not only a better professional, researcher, and academic, but also a better human while making my family proud of what I have achieved.

1.6 THESIS OVERVIEW

This section aims to guide the reader through the structure of the thesis while explaining its rationale. This thesis is divided into seven chapters: introduction, two literature review chapters: ‘the dynamics of donation’ and ‘conceptualising privacy’, methods and methodology, results, analysis, and, lastly, discussion and conclusion.

The present chapter introduces the researcher, the contribution of the research, and provides the reader with the background and context of the phenomenon being studied. The next chapter pertains to the dynamics of donation. As this thesis’ topic focuses on the donation of everyday data, a novel form of donation, the first step warranted the conceptualisation of this type of donation. Accordingly, the second chapter discusses the different types of traditional data donation, introduces the different characteristics of data and articulates the concept of data in relation to the other types of donation. This provides the reader not only with specific information related to how data donation is conceptualised in this research, but also provides a first account of a definition of this concept. Additionally, after introducing and defining the phenomenon studied, the chapter continues by exploring donation. In specific, it provides the reader with an in-depth account of the motivations and risks an individual may experience when deciding whether to donate.

From here it is noted that exploring the concept of data donation would not be complete without exploring its privacy implications. The decision to explore privacy as an extra dimension does not solely stem from the fact that data, as the asset being donated, may

have privacy implications of donating one's data. It is also due to the fact that, when exploring how individuals experience the risks of traditional donation, privacy and information flow seemed to appear as influencing decisions, although this was not addressed by the literature reviewed. Therefore, to investigate data donation, one has to consider the implications that data brings to the potential donors. In other words, investigating data donation, and the potential risks associated, warrants an exploration of the privacy dimension that data adds to the broader phenomenon of donation.

The third chapter conceptualises privacy by exploring how it evolved from different individual-centric approaches to a notion of privacy as having an embedded social value. This chapter explores what type of data can be donated, the potential attitudes of individuals towards data donation, how individuals may be concerned about their personal boundaries, about preserving their relationships, identity, and autonomy, about how their data can be used in different contexts beyond what they initially consented to. Solove's (2006) privacy-harms taxonomy, which, by itself, is rich in sociality, may provide answers regarding what privacy harms people may experience, express, and feel when donating their personal data.

At this point it is noted that there are two dimensions in data donation: data donation as a type of donation; and data donation as having privacy implications. Therefore, this research investigates how these two dimensions interplay in the subjective domain of risk construction. In other words, how do individuals construct the risks associated with donating their personal data? Accordingly, this thesis addresses the different layers composing data donation and explores their interplay.

After concluding the third chapter with the research question being addressed in this thesis, the methodology and methods chapter discusses the research philosophy adopted and explores how the research question is going to be investigated. Namely, it examines the adoption of social constructionism as a research paradigm, and the choice of focus groups as the best suitable method to address the research question. It also discusses the introduction of vignettes as stimuli for the group discussion. Lastly, it considers the structure of the focus groups and the questions asked.

After the data collection and analysis of the generated data takes place, the results chapter presents the coding structure derived providing the rationale as to why I decided to ascribe certain codes to given arguments. Subsequently, chapter 6 analyses the data and discusses the interplay between risk frameworks and risk perception, intensification and mitigation.

Lastly, the concluding chapter discusses this research's empirical and theoretical contributions, together with the limitations and policy implications of this thesis. Namely, it addresses how the findings add to the donation and privacy literature.

Chapter 2: THE DYNAMICS OF DONATION

2.1 INTRODUCTION

This chapter provides the reader with an introduction and discussion of the concept of donation and its impact in society, together with a first account of everyday data donation as another type of donation. This chapter considers the different aspects of the donation process, including the characteristics of the different types of assets donated, and how existing research about these different types of donation may contribute to the understanding of data donation.

This chapter starts by presenting the different traditional types of donation, such as monetary, blood, organs, products, time, and medical data. It discusses relevant literature on each type of donation. It follows by presenting what is known so far about data donation, especially referring to the context of medical data, as this is the only area where data donation is mentioned. A discussion of the characteristics of data and how these may compare to the characteristics akin to the other types of donation follows, in order to understand what makes data, and, in consequence, data donation, unique from any other asset.

It is essential to explain the distinction between data donation and data sharing, as the two concepts can initially seem very similar. The distinction between data sharing and

data donation culminates in the proposal of a definition for the term ‘data donation’. The distinction between these concepts, as well as the definition of the concept of data donation provides guidance to the reader and sets the context of this research. It also helps the researcher guide the participants so that they can distinguish data donation from data sharing and understand what donating data might entail.

After discussing the different types of donation and conceptualising data donation, the chapter moves to discuss why individuals may be interested in donating their data, supported by Deci and Ryan’s (1985) Self Determination Theory (SDT). This specific section divides the different types of motivations depending on their source: intrinsic or extrinsic. Focusing on the motivations behind individuals’ decisions to donate helps to understand the subjective issues and nuances that can affect the way individuals understand data donation.

This chapter concludes by exploring what may deter individuals from donating, according to Barkworth and colleagues (2002) work on adapting Mitchel’s (1999) consumer risk perception framework to the context of donation. After looking at motivation, the decision to turn to risks is not one to oppose positives and negatives of donation as if the difference between them would indicate one’s willingness to donate. Instead, this chapter aims to capture the complexity and subjectivity of the decision-making process. Although one might notice a hint of trade-off narrative present throughout the structure of the chapter in that motivations and risks are presented as antitheses, this does not constitute this research’s unit of analysis. This thesis is

focused on a more socially embedded phenomenon, as explored in subsequent chapters.

2.2 TYPES OF DONATION

When one thinks about the concept of donation, data is not usually the first thing that comes to mind. Instead, there are other types of donation that an individual may consider before even thinking of data as something that can be donated. Donating money, blood, organs, products or time (volunteering) are more traditional forms of donation. Even when data is considered as a type of donation, one usually thinks about the donation of medical data for research (a one-off event), not in the donation of data generated during the course of everyday life.

Accordingly, this section introduces these different traditional types of donation: monetary, blood, organs, products, time and medical data in order to establish how data donation can be considered a distinct and unique phenomenon. It starts by introducing some key figures and statistics and continues by discussing the importance of that type of donation, together with how the need for it is communicated. As the types of donation covered are so vastly different, points of comparison need to be set out. For example, donating money to a homeless individual is different from donating a kidney or volunteering at an institution. There are differences between money, organs, and time as the assets being donated in this example. These differences are not only related to the different characteristics of these assets, but also how the process of

donation takes place, how the need for these donations is communicated, amongst other things.

Similarly, donating everyday personal data may also differ from the other types of donation as the characteristics of data vary from the characteristics of the other types of assets that can be donated. Thus, the need to set out terms of comparison between the different types of donation here discussed: to understand what makes everyday data donation unique when compared at the other types of donation. These terms of comparison are based on Levitin and Redman's (1999) discussion of the characteristics of data. Namely in reference to data's tangibility, consumability, shareability, copyability, transportability, fungibility, fragility, versatility, valuation, renewability, and storage. These can be observed in table 1.

Below, the chapter follows by considering the different traditional types of donation, starting by the donation of money.

2.2.1 MONETARY DONATION

The Charities Aid Foundation (CAF, 2019) reports that, in 2018, 57% of British population donated money to a charity, and, of those, 51% have done so by recurring to 'GiftAid'⁶. This figure represents a 61% decline in number of donors in 2016.

⁶ GiftAid pertains to the automatic deduction of a portion of an individual's tax returns and it is the most popular way of donation money in the U.K.

Despite this sharp fall in donors, the figures relating to the proportion of donors giving by 'GiftAid' remained consistent with previous years.

During 2018, an estimated amount of £10.1 billion were donated, with an average of £45 donated per individual. Furthermore, 26% of the monetary donations were made to animal welfare, as well as to children or young people's causes (26%), followed by medical research (25%) and hospitals and hospices (20%). However, despite the loss in donors, when compared to 2016, the total amount given to charity in 2018 increased by £400 million, to £10.1 billion. According to the Charities Aid Foundation's (2019) report, monetary donations remain the most popular form of giving.

The fact that monetary donations are one of the most popular type of donations may be attributed to its simplicity and relatively low risk. For instance, it is possible to donate through the internet (Talbot, 2008), by setting up a direct debit (Redcross, 2018), by deducting from one's salary, commonly known as 'payroll giving' (Leigh and Finelli, 2004), by automatically deducting a portion of one's tax returns, commonly referred as 'GiftAid', (Cooter and Broughman, 2005) or simply by giving cash (Gaetz and O'Grady, 2002). The majority of these processes, apart from cash donation, once set, are practically automated. The donor does not need to actively participate in the donation process as it would, for example, when donating blood (Sundeen, Raskoff and Garcia, 2007).

2.2.2 BLOOD DONATION

According to the National Health Service Blood and Transplant (NHSBT, 2020) there is a need for around 135 000 new donors per year as some donors are no longer eligible to give blood. According to the NHSBT's (2020) figures, during the 2019 - 2020 period there were 416 381 new donor registrations, a considerable decline from the previous year's figures of 509 000 new donors. In addition, the fact that the blood's main components have a short shelf life (e.g. red blood cells have a 'shelf life' of 35 days, platelets up to seven days and plasma up to three years) enhances the need for more frequent donations (NHS, 2017; WHO, 2018). The World Health Organisation (WHO, 2018) states that roughly 112.5 million blood donations are collected around the world. In the UK, during 2019 - 2020, of roughly 1.3 million registered blood donors, only 807 805 donors gave blood, a steady decline of over 80 000 donors since the 2015 – 2016 period (NHSBT, 2020).

In regard to how the need for blood donations are communicated to the public, messages are, typically, altruistic, suggesting that giving blood saves lives (Ferguson, Farrell, and Lawrence, 2008; Guardian UK, 2015; The Sun, 2017; NHS, 2017). In fact, donating blood is often seen as an altruistic behaviour (Ferguson, Farrell, and Lawrence, 2008). Nonetheless, and despite the fact that 'altruism' is often argued to describe the act of blood donation, and indeed many other forms of donation, this research will debate, later in this chapter (section 2.5.1), whether there is such thing as 'pure altruism'.

2.2.3 ORGAN DONATION

According to the NHSBT (2020), due to low stocks of suitable organs more than 372 patients died during the 2019 – 2020 period while waiting for a transplant. As of February of 2020, roughly 3,100 individuals are waiting for a suitable organ to become available. Moreover, the NHS (2017) reported that 50,300 people are currently alive due to organ transplants. Of these, 36,300 people received kidney transplants, followed by 9,800 people receiving liver transplants. It is important to note that due to recent legal changes⁷ these figures can dramatically change over the next years.

Depending on the organ its donation can be done while alive or *post-mortem*. However, donated organs are not necessarily transplanted to individuals who need them. They are also often donated to research institutions. The donation of organs to science happens, in general, with organs that are not transplantable, such as the brain (U.S. Department of Health, 2016).

How the need for organ donors is communicated is a little challenging. Despite the fact that these communications also have altruistic substance (see Morgan and Miller, 2002; Hill, 2016) it is very hard for the donor to conceive the process of donating an organ. If live donating an organ, such as, for instance, a kidney, it is a laborious, time-consuming process that would entail the donor to be under anaesthesia, bear some

⁷ “All adults in England are now considered potential organ donors, unless they choose to opt out or are in one of the excluded groups” – NHS (2020) England now operates on an ‘opt out’ system.

degree of pain and likely admitted to hospital for several days (see Gill and Lowes, 2008). As expected, it is not a decision that is taken as lightly as any other form of donation, especially as it carries significant risks (Lentine and Patel, 2012). Furthermore, deciding to donate organs *post-mortem* is equally a very hard decision to make. It may, for example, go against an individual's religious beliefs. Due to the pressing need for more organ donors, and due to the complexity of influencing new individuals to register as donors, many countries are now pursuing an opt-out system instead of opt-in, as is recently the case of England⁸.

2.2.4 PRODUCT DONATION

According to the Charities Aid Foundation (2019), the donation of products is the second most popular type of donation. Just over half of the British population reported donating some sort of good to a charity in 2018. In fact, the donation of products, such as books, clothes, and food are often viewed not only as prosocial behaviour but also as a way to ethically dispose of the products an individual no longer uses (Ha-Brookshire and Hodges, 2009).

When it comes to donating food, a type of product donation, food banks are responsible for collecting, storing and distributing non-perishable items (Schneider, 2013). Conversely, food rescue programmes (e.g. soup kitchens, shelters) commonly

⁸ <https://www.organdonation.nhs.uk/helping-you-to-decide/about-organ-donation/faq/what-is-the-opt-out-system/>

collect perishable and ready-to-eat meals as they focus on providing hot meals to the hungry on a daily-basis (Feeding America, 2011). During the course of time, the food relief system's task has changed from supplying critical relief to the ones struggling to avoid hunger during the 1960s to provide continued support over a longer period of time from the 1990s onwards (Verpy et al., 2003). There are over 2000 food banks in the UK (Tyler, 2020). According to a report by The Trussell Trust (Sosenko et al., 2019), up to 2% of U.K. households relied on food banks during the 2018 – 2019 period. From the households using a food bank, 14% of them had at least one member in employment. Nonetheless, the most common source of income from an individual using a food bank was state benefits. The average weekly income of individuals referred to a food bank, after paying for any housing costs, is of £50, with 20% of individuals reporting no income at all the month before. Well over 1.5 million food parcels were distributed by food banks during the 2018 – 2019 period. Moreover, some of the risk factors for being referred to a food bank include low income, having more than two children, being a working age adult, lone parent, social renter, unemployed, and living in a household affected by ill health (Sosenko et al., 2019).

Product donation, especially food donation, has a striking impact in people's lives. Individuals who are in difficult conditions, who experience hunger and food insecurity, rely on these donations to meet an essential biological need. Especially now, at the time of writing, when a pandemic sweeps across the world and families experience moments of extraordinary hardship, food banks, and other charitable institutions offer the critically needed help for households to make ends meet. According to the Trussell Trust (The Guardian, 2020), during the last two weeks of March of 2020, food banks

in their network distributed over 40,000 more food parcels than the previous analogous period.

Not every product donation comes from individuals. Increasingly, companies are implementing the donation of products into their corporate social responsibility (CSR) policies (Schneider, 2013; Garrone et al., 2014). A study by Scherhauser and Schneider (2011) concluded that 3.3% of the leftovers of bread and pastries are donated to charitable organisations while the rest goes to waste. In 2020, the Waste and Resources Action Programme (WRAP), reported that, annually, in the UK, an estimated 4.5 million tonnes of food and drink are wasted. Actions to raise the awareness of this issue are taking place. In 2019, over 100 companies operating in the British food sector signed a government pledge to reduce their food waste⁹. All of the UK's biggest supermarkets signed this promise. These companies, amongst other things, pledged to help halve food waste by 2030. Furthermore, in recent years apps such as 'too good to go' have become popular mechanisms to help the industry reduce their food waste¹⁰.

2.2.5 TIME DONATION (VOLUNTEERING)

In the UK, during 2018, one in six people donated their time (i.e., volunteered) to a charity. Students and part time workers have been the most common volunteers,

⁹ <https://www.gov.uk/government/news/slashing-food-waste-major-players-urged-to-step-up-to-the-plate>

¹⁰ <https://www.theguardian.com/environment/2019/jul/06/food-waste-how-to-get-cheap-grub-and-help-save-the-planet>

perhaps due to their availability (CAF, 2019). These volunteering opportunities can take many forms, ranging from working on the charities' frontline by helping them with, for example, fundraising, sales, or preparing and delivering food, to more technical volunteering, such as employing their technical skills (e.g. marketing support).

The need for volunteers, similar to the need for other types of donors (e.g. blood and organ donors) is communicated by using implied altruistic messages. For instance, “A charity working to help keep seniors and dogs together is looking for more volunteers”¹¹; “Indiana food banks need volunteers or will cut hours”¹²; “We need one million more volunteers for the COVID-19 vaccine trials”¹³. These messages try to appeal individuals to help a cause by donating their time to it. Whether it is spending time helping ‘keep seniors and dogs together’, or spending time helping food banks stay open, or take part in helping discover a suitable vaccination for SARS-CoV-2, these communications convey an altruistic message. If prospective volunteers are motivated by these altruistic messages, or perhaps other intrinsic or extrinsic motives, will be discussed in section 2.4.

¹¹ <https://www.castanet.net/news/Penticton/312398/A-charity-working-to-help-keep-seniors-and-dogs-together-is-looking-for-more-volunteers>

¹² <https://eu.indystar.com/story/news/2020/10/02/indiana-food-banks-need/3563324001>

¹³ <https://time.com/5894798/need-volunteers-covid-19-vaccine-trials>

2.2.6 MEDICAL DATA DONATION

The donation of medical data is not a novel phenomenon when compared to the donation of everyday data. Medical data is typically collected by a health professional during the course of a medical examination or lab testing, and it is then associated with the patient's medical record. The patient can allow the hospital or any other entity to make use of their medical data for research purposes. For instance, the medical data of an individual who was infected by SARS-CoV-2 can support research in understanding how the novel virus interacts with one's immune system¹⁴.

The availability of blood and organs, for example, are often the difference between life and death for many people. When it comes to medical data, however, as there are often exceptional circumstances in which these types of donation take place (e.g., data donation for researching a cure for a certain disease), decision-makers are precluded from advancing an ethical, legal, and regulatory frameworks that would make the donation process easier (Krutzinna and Floridi, 2019).

Figures pertaining to the amount of data that is donated for medical purposes is challenging to find. Huser, Miller and Vawdrey (2014) found that the Marshfield clinic in Wisconsin, by 2056, will have more data about deceased people than living patients. It is unequivocal that there is a wealth of data that is ready to be donated for medical purposes. A study by Mello, Lieou, and Goodman (2018), found that 93% of

¹⁴ <https://www.data4life.care/en/journal/data-donation-in-medicine/>

participants (n = 771), would be willing to give their medical data to scientists. So why is this practice not so widespread? Krutzinna and Floridi (2019, pp. 2) argue that “researchers are increasingly encouraged – and sometimes even required - to share their data in the name of science, and yet individuals cannot easily make their data available for scientific purposes. This presents an ethically unjustifiable asymmetry [...]”. For example, blood test results, heart rate data, electrocardiogram (ECG) data, doctor’s notes about the patient, can be used to expand knowledge about a given disease, and thus support the development of more efficient treatments (Safran et al., 2007). A more concrete example of this is the ‘Corona Donation App’ initiative in Germany¹⁵. As of the end of September 2020, the initiative had over half a million users connecting their wearable devices to the app. The collected data, together with data from research institutions, hospitals and other data sources, helps researchers understand patterns in the symptomology, disease development, its impact in the individuals’ heart rate, its spreading pattern, amongst other things. A similar project, also in Germany, asked for citizens to donate their data to help understand and identify early signs of a COVID-19 infection¹⁶. The use of data collected from wearable devices to identify and improve surveillance of ‘influenza-type’ illnesses was studied by Radin and colleagues (2020). Figure 2 below illustrates the process and dynamics of medical data donation.

¹⁵ <https://corona-datenspende.de/science/en/reports/>

¹⁶ <https://fasterthancorona.org/>

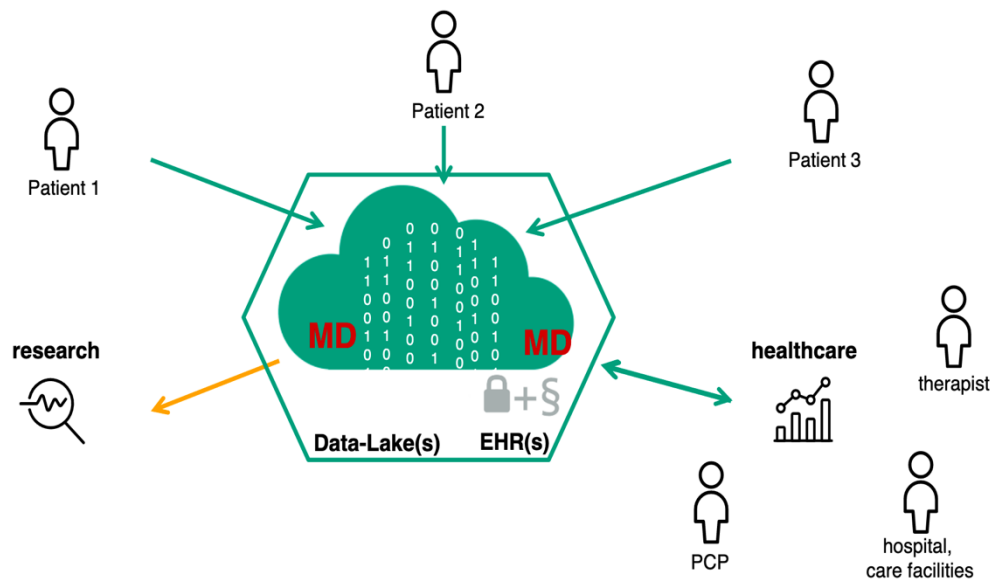


Figure 2 - Dynamics of Medical Data Donation

Source: Klucken (2020)

In regard to how the need for medical data donations is communicated, discourse is often centred on the advancement of scientific knowledge, that may lead to scientific breakthroughs in treating illnesses, as the examples illustrated above. A comparable reasoning to that of blood or organ donation can be observed, although without the immediate lifesaving consequence of the latter types of donation.

The donation of medical data has been around for decades. However, the type of donation this thesis investigates, encompasses a different sphere of data donation. A more mundane, ordinary, type of data donation, where individuals can make use of new technologies and devices to donate their everyday personal information to, for example, their local governments. Accordingly, this research moves past these ‘one-off’ donation scenarios to focus on a more every day, recurrent type of data donation. However, what is it meant by everyday data and how is it different from medical data? Medical data is all data that can be collected by a health care system for the purpose

of understanding and treating an individual's ailments. To this category pertains data that is connected with an individual's bodily functions, physiology, illness history, doctor's notes, amongst other things. For instance, blood tests, electrocardiograms (ECGs) are considered examples of medical data. When considering 'everyday' data, one is referring to the data generated by individuals during the course of their daily life. For example, speed data, itinerary data, location, amongst other things. Nonetheless, some medical data can be considered 'everyday' data, and vice-versa (e.g., heart rate data). The difference between 'everyday' data and medical data will then be understood based on what is the data used for. If heart rate data is used in a medical context, then it is said to be medical data, if it is used to provide insights to the subject about their last run, and overall fitness levels, then it is considered everyday data.

After establishing what is medical data donation, and the difference between medical data and everyday data, the following section explores the difference between data donation and the other types of donation previously discussed. Specifically, it investigates what makes data donation so distinct from the traditional types of donation.

2.2.7 DATA AND THE TRADITIONAL TYPES OF DONATION

After discussing the different types of traditional donation, this section explores what makes data donation unique when compared to the other types of donation, based on Levitin and Redman's (1998) categories. This distinction is important as it establishes

the uniqueness of data donation and, thus, points out the importance of exploring data donation as a separate type of donation. Additionally, it sets out how everyday data donation differs from medical data donation and the other types of traditional donations. Levitin and Redman (1998) presented data as a resource, identifying and discussing some of its characteristics, in no particular order: tangibility, consumability, shareability, copyability, transportability, fungibility, fragility, versatility, valuation, renewability, and storage. Similarly, it is also possible to ascertain the characteristics of the other types of donation based on these authors' categories.

First, the authors claim that data can be considered tangible as one can print it and physically touch it. However, as twenty years have passed since the introduction of these characteristics of data, and as cloud computing is becoming ever more prevalent, the need to print a dataset is now diminished. Accordingly, in the context of this research, data are distinctly intangible. Time (volunteering), as with data, is also distinctly intangible. Money, blood, organs and products are all tangible assets.

Second, data are non-consumable as their usage does not decrease the amount available to the owner. Blood has similar characteristics in that the amount of blood in the donor's body is not reduced (in the long term) with the donation given that it is quickly restored by the body (within 6 to 12 weeks)¹⁷. Unlike data or blood, money, products and time are consumable assets. For example, if one spends a given amount

¹⁷ <https://www.blood.co.uk/the-donation-process/after-your-donation/how-your-body-replaces-blood/>

of money, eats a certain amount of food, or spends their time doing something the total amount available of that given asset decreases.

Third, since more than one user can have access to the same set of data at the same time, it can be considered shareable. Products have similar characteristics. For example, a toy can be shared between kids. On the contrary, for example, money, organs, or time cannot be considered shareable. Once given, the donor loses possession of those assets. When it comes to determine the shareability characteristic of blood, however, it becomes conceptually complicated. Donated blood can be used by more than one person, and the donor's body replenishes the amount given. Therefore, whether blood is shareable is not established.

Moreover, data can be copied, as well as transported, with relative ease. Money, unlike data, cannot be copied. In fact, it is even illegal to do so. However, its transportation can happen with ease either through a wallet, briefcase, or electronically, through banking services. Blood and organs cannot be easily copied, although advancements are being currently made in this field (Patel, 2016), and their transportation is a very complex process. Time as an asset that can be donated is distinctively impossible to copy and transport.

Furthermore, a category of data is not fungible as it cannot be substituted by another category of data. Organs share the same characteristic in that one organ, for example, cannot be easily substituted by the same organ from another individual as often this is a complex process tied to a number of compatibility tests. Even if determined that

organs are compatible, the beneficiary has to take immunosuppressants to avoid their immune system from rejecting the new organ, and the transplanted organ's functionality rarely exceeds 30 years¹⁸. Money and products can be considered fungible as, for example, one euro holds the same value as another euro. Similarly, blood is considered to be fungible as it is easily replaced by the body (Carsten, 2013). In other words, the total amount of blood in the body will not permanently decrease after being donated as the body works to replenish the amount that was taken. Whereas, for instance, if the information corresponding to an individual's date of birth is accidentally deleted, this cannot be substituted by data concerning the individual's gender. However, if copies have been previously made, data can be easily replaced by searching for the relevant information in its copy. Time cannot be considered fungible.

The authors also claim that data is fragile as it can easily be destroyed. Nonetheless, as their framework was published 20 years ago, and with today's developments of cloud and other backup technologies, it is sensible to assume that data is not as fragile as once considered by Levitin and Redman (ibid) and cannot be easily destroyed. Monetary assets, assuming that they can be safely managed through a bank account cannot be considered fragile. However, when considering a £5 note, then one may assume its fragility. In contrast, for example, blood, organs or even alimentary products can be considered very fragile. In the case of blood and organs, their shelf life is short.

¹⁸ <https://wexnermedical.osu.edu/blog/how-long-do-transplanted-organs-last>

Versatility, another of Levitin and Redman's (1998) characteristics, relates to the ability data has to perform different functions or to be used in different contexts. Money, as with data, can also be used in different contexts, for different situations. Organs, blood, and to some extent, products have a limited number of purposes and contexts in which they can be used.

Valuation, another of Levitin and Redman's (1998) characteristics, refers to the ability one has to stipulate the value of a resource in monetary terms. They argue that it is hard to assess the value of data in monetary terms as it is dependent on the context that it will be used for. The monetary value of organs or blood cannot be ascertained as they are not commercial assets¹⁹. For someone who needs blood transfusion or an organ transplantation, the value of these assets is inestimable. In contrast, for instance, the value of money or products, can easily be assessed. When considering time, who has never heard of the ever so popular aphorism professed, originally, by Benjamin Franklin (1748): "time is money"? Becker (1965), on the theory of the allocation of time, associates the value of time with its opportunity cost. In fact, Becker's (1965, pp. 494) goal was to include "the cost of time on the same footing as the cost of market goods". Kahneman and Tversky (1979) agree with Becker's argument, adding that the value of time is conditional on different contexts.

Finally, data can be renewed and stored with ease. Especially, over twenty years after their framework was published, data can now be stored in a plethora of ways powered

¹⁹ In some countries, donors may be paid to donate blood and organs.

by different technologies, such as cloud computing and the blockchain. These technologies make the storage of data simple and practically indestructible. Similarly, blood can be easily renewed, as discussed above, however, its storage is complex. The storage of organs is also a complex endeavour in that they have to remain under special conditions in order to keep their utility. These cannot be renewed. Money and products can be renewed and stored with relative ease, except in the case of some products, especially those which are perishable.

This section, so far, introduced and discussed the characteristics of data in comparison to the characteristics of the traditional assets that can be donated. Below, Table 1 summarises this comparison, highlighting the differences and similarities between the different types of donation.

	Data	Money	Blood	Organs	Products	Time
Tangibility	No	Yes	Yes	Yes	Yes	No
Consumability	No	Yes	No	N/A	Yes	Yes
Shareability	Yes	No	N/A	No	Yes	No
Copyability	Yes	No	No	Hard	Yes	N/A
Transportability	Yes	Yes	Hard	Hard	Depends	N/A
Fungibility	No	Yes	Yes	No	Yes	N/A
Fragility	No	No	Yes	Yes	Depends	N/A
Versatility	Yes	Yes	No	No	No	N/A
Valuation	Hard	Yes	N/A	N/A	Yes	Yes ²⁰
Renewability	Yes	No	Yes	No	No	No
Storage	Yes	Yes	Hard	Hard	Depends	No

Table 1 - Comparison Between Data and Traditionally Donated Assets
Source: The Author

²⁰ as per Becker, 1965 and Kahneman and Tversky, 1979

As noted, data has a specific set of characteristics that make them distinct from any other type of donation. In contrast with the other forms of donation, the fact that data can be easily copied, enhances the risk of its unwanted proliferation. In addition, data is a versatile asset that can serve many purposes (e.g., same set of data can be used for health research or for user profiling). Finally, data can be shared. Unlike other types of donation, a variety of people can have access to the same data, at the same time, from different locations.

Due to these distinctive features, two important questions arise: ‘If data are easy to share, copy, transport and store are people donating their data or simply sharing it?’ and, ‘why is the question of donation important?’. The answer to the first question is that it depends on how and why the data is transferred. This is discussed in greater depth in section 2.3, below. Second, the question of donation, and the importance of separating the concepts of sharing vs donation becomes critical in that it helps to understand the underlying motivations, and risks, associated with the different types of personal data collection.

The distinction between data sharing and data donation is one worth making as individuals may have different expectations when donating their data in comparison to sharing their data. For example, an individual may expect to receive promotional coupons should they share their data with a retailer. If, however, they donate their personal data, they might expect it to have a wider social benefit. More specifically, for instance, due to the COVID-19 pandemic, several governments asked individuals to self-identify in an app as carrying the novel coronavirus (e.g., Protect Scotland App

or the Portuguese StayAway Covid App). In this case, the individual is donating their personal data, such as health and location, that may become a source of life-saving information for others. In this particular case there may be different motivations and risks individuals may experience when considering whether to take part.

The literature has so far evidently ignored the difference between both concepts, fitting everything into one pot, while accounting for the only type of data donation as the donation of medical, and related data for research purposes. Nonetheless, it was ascertained that data donation and sharing are two different phenomena, with different dynamics, involving different individuals' behaviours, different social processes and norms and, therefore, should not be studied as if they were the same thing. The section below explores these two concepts in detail and provides a first documented attempt in defining everyday data donation, while suggesting three key parameters to help distinguish data sharing from data donation.

2.3 DEFINING DATA DONATION

After discussing the different types of donations and how data donation compares and differs from these, this section now explores the differences between data sharing and data donation while arguing towards a definition of everyday data donation that is currently lacking in the donation literature. The tension between these concepts (data donation and data sharing) became evident during the last section, thus warranting a further exploration so that an acceptable definition of data donation can be derived.

Data is a unique type of asset. In contrast with, for example, money or blood, data can be easily copied, and cannot be consumed, thus the amount available remains the same. Moreover, as discussed, Levitin and Redman (1998) define one of the properties of data as ‘shareable’ since more than one user can have access to the same set of data at the same time. Consequently, the distinction between whether an act of giving personal data is considered data sharing or data donation becomes distorted. However, with the implementation of the General Data Protection Regulation (GDPR), even though one may have access to another person’s data, the data subject is still the owner of that data (Recital 7, GDPR). Also, the GDPR contends that an individual can request all their personal data held by a third party and ask for it to be permanently deleted from their servers (article 20, GDPR). Even though subject access rights have existed for decades (e.g., UK’s Data Protection Act 1998²¹), an individual is now, unequivocally, the owner of their personal data. Therefore, they can request it from the institution collecting it (e.g., Facebook), and gift it to another (e.g. city council), thus giving rise to a transference of property (Shaw, 2019). Furthermore, there is the assumption of proactivity in giving (Siddiqui and Tee, 2019), and there is the notion of an ultimate goal of a wider good (e.g., Bishop, 2018), two other actions that characterise the act of donation.

With the recent introduction of the General Data Protection Regulations (GDPR), individuals have increasing control over their personal information. However, requesting their personal data, and transferring the ownership of it, is a complex task,

²¹ <https://www.legislation.gov.uk/ukpga/1998/29/contents>

requiring some literacy and proactivity: it is not a straightforward process. Therefore, many institutions, like smart city projects, opt by asking the participant to download an app that continuously collects their personal data, as a form of donation. One might compare this to, for example, monetary donations by direct debit, that, once set up, the donor effortlessly and regularly donates to a charity. Ergo, for an act to be considered data donation it has to fulfil three essential criteria: 1) The donor should proactively acknowledge the transfer of personal data; 2) The data must be formally requested and not simply collected; 3) The recipient of the data should be acting and using the data for a wider social benefit. For example, when Facebook prompts users to acknowledge and consent that their data will be given to a third party by clicking on the button “I agree”, under this definition, it is not an act of data donation, but data sharing. Although there is an act of proactivity by clicking the button (1), and there is a request by the third-party institution (2), the ultimate goal of the data broker or data user is profit. *Accordingly, data donation can be defined as the act, by the data subject, of voluntarily allowing their personal data to be transferred to a third-party that is requesting it, with the objective of promoting public good or for wider social benefit.*

Skatova and colleagues (2014; 2019) attempt to discuss this recent form of donation, focusing on individual motivations: Skatova and Goulding (2019, pp. 3) argue that “donating personal data, similarly to the way we donate blood, could become a new act of digital economy prosocial behaviour”. However, they miss the point of data donation by narrowing its scope and arguing that ways should be found to “encourage and enable individuals to donate their digital footprint for academic research” (ibid),

including health research. In spite of the potential breadth in donation activities implicit within the notion of ‘digital economy prosocial behaviour’ Skatova and Goulding (2019) limit their examples in the scope of medical data donation. With data running through many, if not all, aspects of everyday life, data donation could encompass a much broader range of contexts beyond medical or academic research. Examples include the donation of personal mobility data to smart cities with the premise of, for instance, improving the road network as illustrated in section 1.1.2. These types of data donation are the focus of this research.

After defining data donation and contextualising it in light of this research, the next section deepens the exploration of donation. Specifically, it discusses the different motivations individuals may have to donate. Although not particular to data donation, it helps build an understanding of how individuals experience different motivations to donate.

2.4 MOTIVATIONS TO DONATE

If, as I argue, data donation is a separate phenomenon from data sharing, and it features a voluntary act of donation, why would data subjects be motivated to donate their everyday personal data? A number of explanations exist as to why people may be motivated to donate data. Deci and Ryan’s (1985) Self-Determination Theory (SDT) suggests that both intrinsic and extrinsic motivations may be at play. Extant research focuses on the intrinsic / extrinsic distinction in relation to conventional forms of

donation and those factors are now discussed. In the following sections, research exploring different motivations to donate is discussed in light of the SDT.

Research which examines the motivations to donate predominantly draw upon Deci and Ryan's (1985) 'Self-Determination Theory' (SDT). They argue that motivations can be categorised based on the variety of reasons which result in a given action. An action is said to be intrinsically motivated if it is driven by the individual's willingness to seek enjoyment, and extrinsically motivated if it derives from the desire for a specific outcome. For example, an individual who donates blood because it will make them feel good because they are helping others is said to be intrinsically motivated. In contrast, an individual who donates blood because, as a registered donor, they may have access to certain benefits (e.g., receiving donor cards²²) is said to be extrinsically motivated. This section maps and discusses the different motivations impacting the individual's willingness to donate based on Deci and Ryan's (1985) framework.

2.4.1 INTRINSIC MOTIVATIONS

Tonin and Vlassopoulos (2013) argue that there are two types of intrinsic motivations to donate: pure altruism and impure altruism. The latter is commonly known as the 'warm glow of giving'. Both are antagonistic concepts. With pure altruistic reasons, donors are motivated only by the interest in the well-being of others (Roberts, 1984;

²² Donor Recognition UK: <https://www.blood.co.uk/the-donation-process/recognising-donors/>

Bergstrom et al., 1986), while with impure altruistic reasons, donors are driven by the positive feeling associated with giving (Andreoni, 1989 and 1990).

2.4.1.1 PURE ALTRUISM

“God is not unjust; he will not forget your work and the love you have shown him as you have helped his people and continue to help them (Hebrews 6:10).”

As the bible passage above illustrates, selfless giving is an integral part of the Judeo – Christian, as well as Islamic, religious tradition. In fact, the practice of Zakat is the third pillar of Islam. Zakat is an Islamic term referring to the obligation a person has to donate a portion of their wealth each year to charitable causes. Although religion and selfless giving has been the focus of extensive scholarly research, not all purely altruistic actions take place due to religious beliefs. For example, internalised social norms may also contribute to altruistic actions. This section starts by discussing studies focused on the connection between religion and altruism, and then moves towards other factors impacting altruistic behaviours.

As many religions advocate the love and care for others, a religious individual's tendency for [pure] altruistic behaviours are not uncommon (Regnerus et al., 1998). Nelson and Dynes (1976) investigate this exact relationship. They surveyed 663 American male respondents, eight months after a city in the southwest of the United States of America had been wrecked by a tornado. The researchers looked at different

levels of religiosity and its relationship with helping behaviours in the aftermath of the tornado. They asked individuals how religious they believed they were, how frequently they prayed, how frequently they attended church, how much importance did they attribute to praying, how often they volunteered at disaster relief institutions, and whether they donated money and/or goods to people affected by the tornado. Ordinary helping behaviour, unrelated to the tornado, such as volunteering work or monetary charitable contributions, from the participants was also assessed. The authors found a relationship between religious beliefs and donation behaviours, both routine and in situations of crisis, as was the case of the tornado. However, these donation behaviours were not dependent on the number of times an individual attended religious services.

Furthermore, a study by Perkins (1992) focused on investigating the link between Judeo-Christian religiosity and altruism. The author collected data from five different English and American colleges and universities. In accordance with Nelson and Dynes (1976), Perkins found a strong relationship between students' religious commitments and their altruistic behaviour. In fact, the author claimed that other socio-demographic factors, besides an individual's religious beliefs, did not demonstrate any level of significance. The author concluded by arguing that the results suggest that religiosity might be one of the most important factors influencing altruistic decisions for young individuals.

Nonetheless, not every altruistic action is performed by religious individuals. Berkowitz (1972) argues that altruistic behaviour may also derive from internalised social norms. The author claims that an individual might act altruistically because it is

the right thing to do in an emergency situation, or simply because they sympathise with the person in need. For instance, a study by Piliavin, Rodin, and Piliavin (1969) had students pretending they were falling either physically ill or drunk in the subway and found that in every single time the student was assisted by a spectator. However, Berkowitz (1972), reviewing this and similar studies, asserted that the high frequency of altruistic actions observed were due to its low cost to the one helping. In contrast, should there be a perceived cost, the number of willingly helpers would decay. For example, he contends that the number of people willing to help a fallen individual in the subway would not be the same as the number of people willing to step in if the person was being attacked.

An individual's mood, another intrinsic factor, can also have an important influence on the decision to help others. Isen (1970) found that the participants who had just successfully completed a task were more likely to help others when comparing to the ones that did not do well. In support of this, Berkowitz and Connor (1966) examined the behaviour of college students who, because they had failed a task, received no prize, found that they were less willing to help. They concluded that success and failure, highly contribute an individual's mood, and therefore, crucially impact their willingness to help.

Empathy is another intrinsic factor that influences pure altruistic actions. Rawlings (1970, pp.173) argues that "as a result of having watched their first partner being shocked, subjects might have anticipated the pain that their new partner would feel and thus, out of empathy, tried to minimise their pain". In accordance with Rawling's

study, Krebs (1975) investigated how 60 individuals reacted to a street busker. Half of the participants were told that they had similar personality and values as the performer, while the other half was led to believe the opposite. Each of these segments were divided in half. One half was told the busker won money and experienced pain as he performed, and the other half believed he was performing skilfully out of their own pleasure. The author concluded that the subjects who believed that they had similar values and personality as the performer and that he/she was experiencing pain while performing, empathise more with him. Specifically, when prompted to make a choice on whether to help the busker at a cost to themselves, the participants who felt more empathetic displayed a higher level of altruistic intentions. As noted, empathy may influence how individuals may experience donation. As observed by Rawlings (ibid) and Krebs (ibid), when individuals empathise with another, they go at greater lengths to minimise their suffering. Therefore, empathy can be argued as being an intrinsic motivator of donation.

Throughout this section, altruism as an intrinsic motivator to donate was explored. It was discussed that individuals may engage in selfless actions due to their genuine interest in others' wellbeing, with issues such as one's religion, mood, empathy as precursors of pure altruistic actions. The next section challenges the notion of 'pure' altruism and explores the idea that altruistic actions are never selfless but instead are rewarded with a 'warm glow' – a positive feeling.

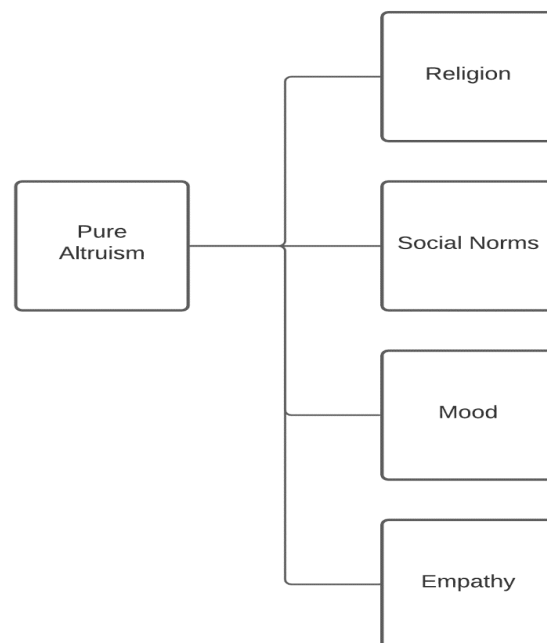


Figure 3 - Factors Influencing Pure Altruistic Actions

Source: The author

2.4.1.2 IMPURE ALTRUISM

Impure altruism, commonly known as the 'warm glow of giving', is another intrinsic form of motivation. Menges and colleagues (2005) assessed individuals' willingness to pay more for electricity as long as this would come from renewable energy sources. The authors surveyed 200 people in Kiel and Düsseldorf, two German cities. The

authors found that participants were willing to pay extra as they perceived increased benefits from cleaner energy and improved environmental quality (i.e., public good). Furthermore, the positive feeling associated with performing socially conscious actions, as is the case of contributing to the protection of the environment, was also reported as a motivation to the willingness to contribute. In other words, individuals' understanding that by switching to a sustainable source of energy would make them feel like they are doing an altruistic act, thus making them feel better, was a contributing factor to their willingness to help.

Crumpler and Grossman (2008) gave 144 participants \$10 each asking them how much, from that amount, were they willing to give to a chosen charity. Additionally, the participants were informed that the supervisor of that study also has \$10 to donate to the participants' charity of choice. However, and most importantly, whatever charity was chosen, the maximum amount donated was of \$10. Therefore, the amount donated by the supervisor would be reduced by the amount of money the participants were willing to donate. For example, if a participant chose to donate \$10, the supervisor would not donate anything. If a participant chose to donate \$7, the supervisor would donate \$3, and so on. With this precondition, the authors aim to exclude other motivations to donate, such as pure altruism - given that no matter what, the charity will receive \$10 - and any extrinsic motivation - given that there is no external motivator to donate. They found that 57% of the participants contributed with at least \$1. In other words, more than half of the participants decided to make some sort of contribution, even though it had no impact on the overall amount the charity would receive. Therefore, Crumpler and Grossman's (2008) study, in accordance with similar

research (e.g., Eckel and Grossman, 1996; Davis et al., 2005; Tonin and Vlassopoulos, 2013, 2014), support Andreoni's 'warm glow of giving' claim that the positive feelings associated with the act of giving are a motivator of an individual's willingness to help.

Nonetheless, it is possible to assert that pure altruism and impure altruism can co-exist. For example, in Crumpler and Grossman's (2008) study one might argue that the participants donated, not only because they seek the positive feeling associated but because they wanted to reduce the financial burden to the supervisor of the study, thus indicating, what can be considered, a purely altruistic motive. Although they may feel good by contributing to the others' well-being, that might not be the only reason. Accordingly, intrinsic motivations derive from pure or impure altruistic reasons. While pure altruistic reasons may be influenced by individuals' religious beliefs, social norms, mood, and empathy, impure altruism focuses on the internal, often psychological, reward one seeks for donating (i.e., the good feeling associated with doing good deeds). Below the intrinsic motivations to donate are pictured.

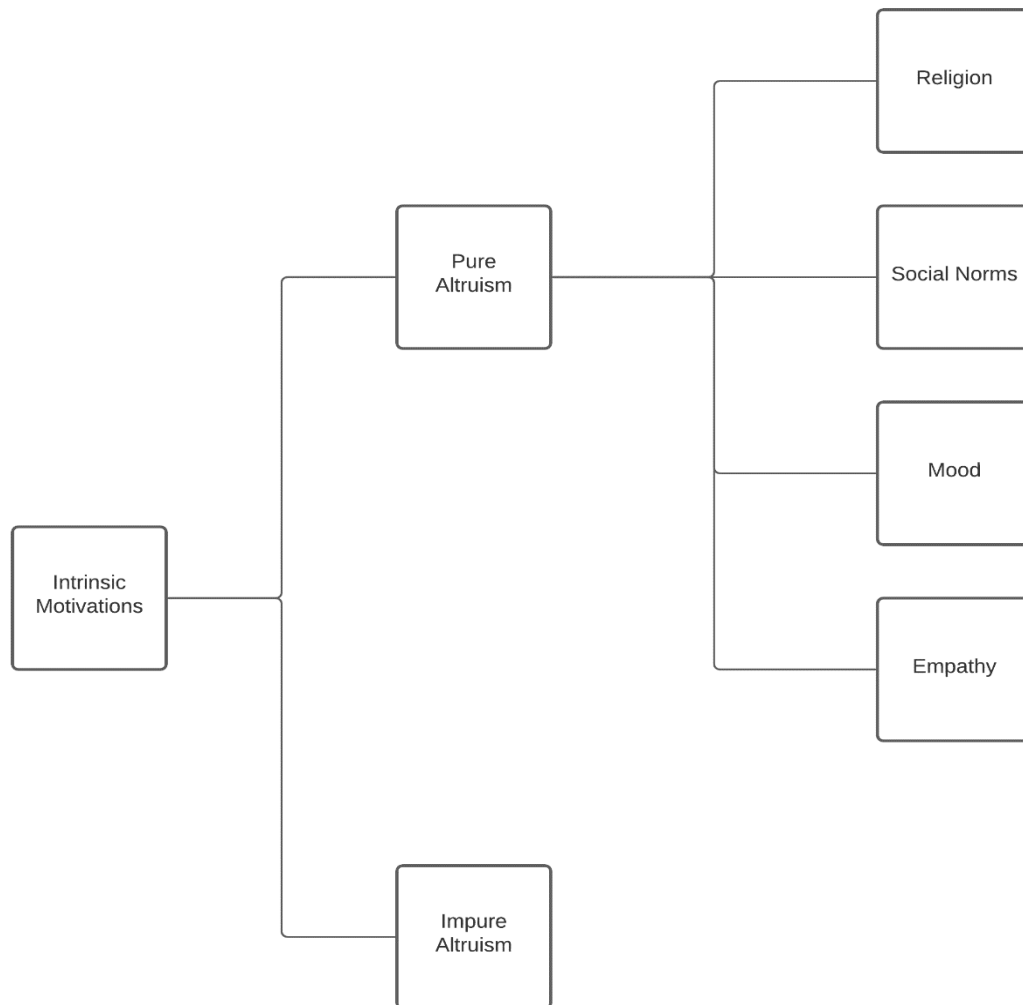


Figure 4 - Intrinsic Motivations of Donation Behaviour

Source: The Author

2.4.2 EXTRINSIC MOTIVATIONS

Extrinsic motivations, according to the Self-Determination Theory, are the external variables that influence an individual to perform certain action. Typically, it may be a reward that one is awarded upon donating their personal data. These extrinsic reasons, in theory, can be a plethora of things, such as, for example, increased reputation, tax

breaks, and discounts in certain products. The extrinsic motivations to donate are now dissected and discussed by distinguishing between intangible, tangible, or both, as is the case of conspicuous donation.

2.4.2.1 INTANGIBLE REWARDS (SOCIAL REWARDS)

The possibility of obtaining social rewards, such as an increase in reputation or social approval may influence an individual's decision to donate. Barclay (2004) investigated how the possibility to earn recognition may impact an individual's giving behaviour. He found that the donations were higher in the group where reputation could be increased by donating money to causes providing a wider social benefit (e.g. charities). This recognition prompted the participants to donate more money during the trust game. In contrast, in the control group, where no reputation could be earned, the donations to similar causes were considerably smaller. The study conducted involved 120 participants.

Bekkers (2010), in agreement with Barclay (2004), argues that an individual who perceives that a donation may result in a high social reward, such as an increase in reputation, is more likely to donate. Conversely, if a given action is associated with a social cost, such as a decrease in reputation, then an individual would be more hesitant in performing it. Additionally, Bekkers (2010) claims that the level of this effect depends on the social distance between the donor and the one who is requesting the

donation. This may be due to the fact that good reputation matters most if it is within one's social group.

Social approval, as with an increase in reputation, helps explain why some individuals act a certain way without an apparent reward. In a study conducted by Izuma, Saito and Sadato (2009), social approval as a motivation to donate was tested using MRI scans. 23 individuals were involved in the study. They were advised that they would be put in a room where an MRI machine would scan their brain while they would be making decisions of whether or not to donate to several different charities. The participants were advised that their responses would be presented on a screen, that there were two individuals observing the participants performance, and that they would be able to see the faces of these two observers. From the 78 real charitable scenarios, the observers were present during half of them, and the participants were aware of this. This way the experimenters could assess if the presence of others may condition an individual's attitude. Additionally, the participants were told that every time they chose not to donate, they would be given the \$5 that would normally go to charity should they have chosen to donate. The authors found that the presence of observers impacted the behaviour of the participants. In fact, when they were present, the participants donated, on average, 33.3 times more. It was also found that the striatum, part of the brain responsible for decision making, among other things, had a higher number of activations. Izuma, Saito and Sadato (2009) concluded by stating that the sheer presence of observers increases one's likelihood to donate.

2.4.2.2 TANGIBLE REWARDS

This section discusses the influence of tangible rewards, such as payments, opportunities or tax breaks, as a motivator for donation. Individuals may be motivated by the possibility of being rewarded for their donation. These tangible rewards can take various forms, such as, for example, tax-breaks or gifts. However, it is possible that, not every type of donation can be influenced by offering tangible gifts. Blood donation, for example, according to the ‘crowding-out’ theory may be the case where incentivising the donation by offering tangible rewards, may lead to an effect contrary to what the institution is expecting.

Falk (2007), in cooperation with a large charitable organisation, sent a total of 9,846 letters to private households in Zurich. The list of addresses was provided by the charity. The study population was divided in three groups and each sent one specific message. In one group, a letter asked for donations and included no tangible gifts was sent (i.e., control group). In the second group, the experimenter sent the exact same letter asking for donations, however, this included a postcard drawn by a child in Dhaka, Bangladesh (i.e., a small gift). To the third group the exact same letter was sent, however, it included a set of four postcards drawn by kids in Dhaka, Bangladesh (i.e., a larger gift). All the recipients were informed that these postcards were drawn by kids in Bangladesh and that they were the beneficiaries of the donations. The author found that in the first group, who received no gift, 12% of the participants donated. In the second group, 14% of the households made a donation, and, in the third group, 21% donated. A 17% increase in donations were observed if a small gift was included

and, 75% when a larger gift was included, thus concluding that tangible rewards influence individuals' donation intention.

Nonetheless, even though Falk's (2007) study supported research which had drawn similar conclusions (e.g., Lange and Stocking, 2009; Gneezy and Rustichini, 2000; Landry et al., 2006), it is important to point a shortcoming in this study. When households were sent a gift, even if small (i.e., only one postcard), there may have been other reasons involved to explain the increase in donation, that were not accounted for or even acknowledged. For example, after seeing that the postcards were drawn by kids in Bangladesh, the beneficiaries of the donation, the potential donors may have felt sympathy. Perhaps neutral gifts could have been sent in order to control for the potential increase in intrinsic motivators.

Similarly, Landry and colleagues (2006) divided 5,000 households into four equal groups. Two of these groups were approached and requested to donate, to a known charity, a voluntary amount of money. The remaining two groups were also asked to donate any amount of money, however, that donation would guarantee their participation in a lottery where they could earn one or more prizes. Consistent with the previous findings, the authors found that gifts, or, in this case, a chance to earn a prize, have a positive influence in the potential donors' intentions to donate. In fact, the number of donors saw a 100% increase from the control groups to the groups where prizes could be won.

However, in contrast, there is a substantial body of literature arguing that offering gifts to motivate an individual's donation may result in the opposite behaviour, also known as, crowding-out. In other words, by being offered gifts in exchange for their donation, individuals may be demotivated from giving, thus the term crowding-out. This concept was advanced by Titmuss in 1970 in his seminal book "The Gift Relationship". In his book, Titmuss (1970) compared the circumstances in the United States, where a substantial portion of blood donors are paid, but the country still faces frequent shortages of blood supplies, with the United Kingdom, where no donor is paid, and shortages are not as common. The author concluded that if blood donation is treated as a commodity, and not as a civic, moral duty, individuals would not be as motivated to donate [blood]. However, the author's 'crowding-out' theory is solely based on the countries blood donation's descriptive statistics and inferences derived, and not empirically tested. Subsequent tests, as for example Mellstrom and Johanneesson's (2008) study did not find statistically significant results that were able to support Titmuss' 'crowding-out' theory.

2.4.3 CONSPICUOUS COMPASSION

The Self-Determination Theory accounts for intrinsic and extrinsic motivations. However, it does not account for more socially embedded motivators as is the case of, for example, conspicuous compassion. This section demonstrates that conspicuous compassion is a socially embedded phenomenon with both intrinsic and extrinsic characteristics that has been shown to motivate individuals to donate.

One can often notice individuals wearing red noses in support of Comic Relief, the remembrance poppy in support of the British Legion, pink ribbons in support of breast cancer, amongst many other symbols representing charitable causes. This can be thought of as an intrinsically motivated act. For example, an individual wears a remembrance poppy to show their support for the cause, and, thus, it is possible to assume that they are not expecting anything in return. However, a phenomenon known as ‘conspicuous behaviour’ or ‘conspicuous compassion’ shows that the motivation causing the purchase of ‘empathy ribbons’ is mainly ostentatious rather than altruistic (e.g., Grace and Griffin, 2006; West, 2004; Grace and Griffin, 2009).

In his book, West (2004) builds the concept of conspicuous compassion from previous work laid out by Veblen (1912) on conspicuous consumption. Veblen (1912) argued that people would consume goods as a way to increase their social standing. Based on this, West (2004) contends that a visual demonstration of compassion may improve an individual’s reputation, thus becoming an extrinsically motivated action. Grace and Griffin (2009, pp. 16) first defined Conspicuous Donation Behaviour as “the act of donating to charitable causes via the visible display of charitable merchandise or the public recognition of the donation”. However, despite this and despite the fact that Grace and Griffin proposed several research directions and ideas and even developed a Conspicuous Donation Behaviour framework (CDB) to assess a donor’s conspicuous compassion behaviour, the issue has remained under-researched.

Rogers (2014) is one of the first researchers to empirically investigate how the purchase of goods that display involvement with a cause (e.g., a charitable t-shirt),

impacts an individual's reputation. A total of 478 participants were recruited and told they were involved in studying a company's merchandise. Different shirts alluring to a charitable cause in the Democratic Republic of Congo were distributed amongst a large part of the participants, and the rest was given a plain white t-shirt. The individuals who received the shirt representing the cause were told the story about that cause and the ones who received a white t-shirt knew nothing about it. The participants were then asked to imagine purchasing that shirt and how would that make them feel. The author found that the individuals who received the shirt alluring to the cause believed they were a 'good person' when comparing to the ones that were wearing a white shirt. Rogers (2014) claims that wearing sympathy symbols, such as ribbons or shirts, signals other that one is a good and compassionate person, enhancing their social standing. Nonetheless, in this study the subjects were wearing a shirt from a cause they knew very little about, and that the general public does not recognise as easily as, for example, other high profile causes such as comic relief or children in need. Accordingly, it may be argued that others would not recognise the charitable involvement of the individual, and thus, not increasing their reputation.

Conspicuous compassion behaviour is present not only through the display of ribbons and other empathy goods, but also through social media. The possibility to create and apply filters on users' profile pictures alluring to their support of a cause, can be taken as an example. Furthermore, the use of hashtags, such as #jesuischarlie, or #stayhomesavelives, demonstrate yet another way to publicly display one's involvement with a given cause or, in support of victims of a disaster. For these reasons, it is argued that conspicuous donation behaviour has hybrid characteristics. Individuals seek to acquire and display tangible empathy symbols (e.g., ribbons) in order to enhance their social standing and reputation. Nonetheless, this may be just an added benefit to an intrinsic motivation that is empathy to a cause or feeling good about helping others.

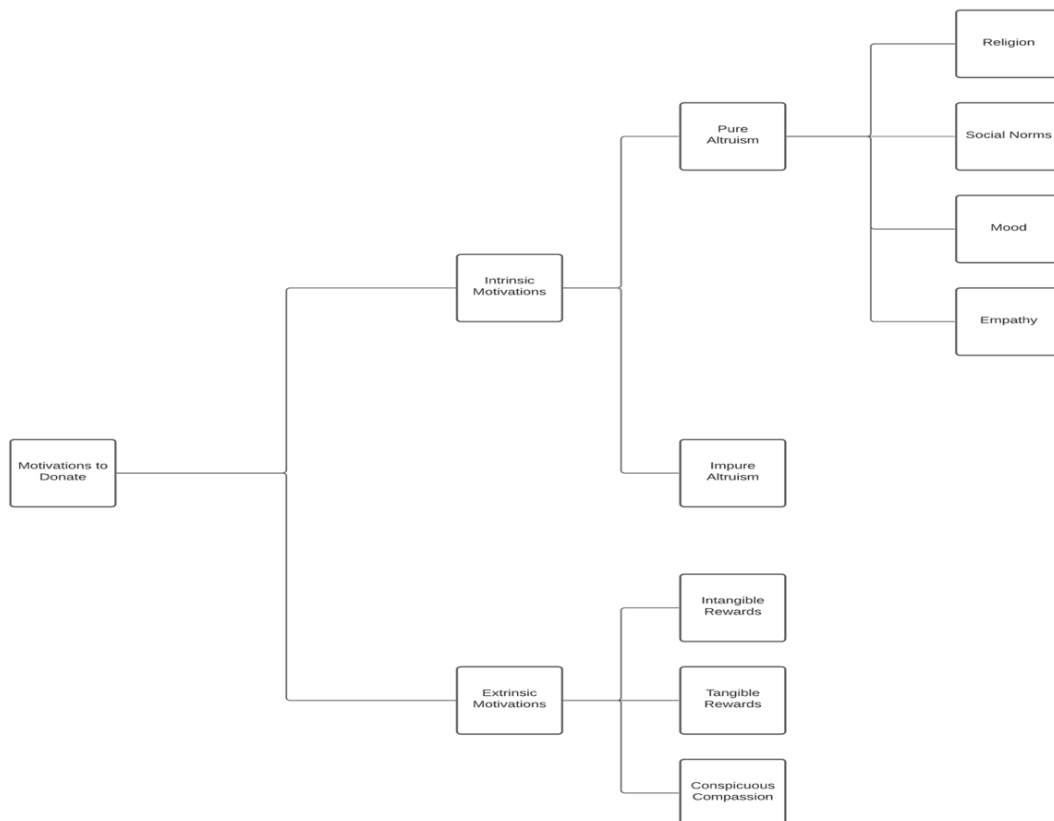


Figure 5 - Motivations to Donate

Source: Author

Despite the fact that the Self-Determination Theory is a widely accepted framework to understand individual motivations, it does not account for more socially embedded motivators, such as conspicuous compassion. Also, it does not account for experienced risks and their interactions with the motivators discussed. Accordingly, the following section, in order to delve deeper into the dynamics of donation, explores the risks individuals may experience when considering whether to donate. These risks are presented as occurring throughout the different types of donation and are not specific to a type of donation. As data donation is so distinct from the other types of donation, are these risks also experienced by individuals who are considering whether to donate their personal data?

2.5 THE FOCUS ON RISKS

Even though there are benefits to donation, there are also risks associated with it. The Self-Determination Theory is an appropriate tool to frame and discuss the possible motivations to donate. However, the SDT does not consider the possible risks associated with donation and how they are perceived by potential donors. Accordingly, it is now important to address this gap by discussing how individuals may perceive the potential risks associated with donation. In order to consider this other dimension influencing why individuals donate, I draw on the work of Barkworth, Hibbert, Horne and Tagg (2002) on the perceptions of risk when considered whether to donate, influenced by Mitchel's (1999) work into risk perception in consumer behaviour.

Barkworth and colleagues (2002) adopt the six main types of perceived risks from Mitchel's (1999) framework to the context of donation. These perceived risks may influence a potential donor's decision to donate: physical risk, social risk, psychological risk, financial risk, performance risk and time risk. Social risk refers to the fact that an action might decrease a person's social standing and status. In other words, if an individual cannot give blood because of health problems, their social group can think it is because of an STD, and, therefore, diminish the potential donor's status. Physical risk has to do with the possibility of a donation causing harm to the donor – for example, pain caused by a needle. Psychological risk is connected to the potential adverse mental effects of a donation – for instance, the anxiety associated with the possibility of an individual finding out they have a life-threatening disease in a blood test. Financial risk is connected to the impact a donation has on a person's financial situation. For example, an individual with a lower income may have a higher perceived financial risk than a person with higher income when it comes to donating money to a charity. Performance risk is associated with the fear of the person or organisation that receives the donation not performing as expected. For example, donating to a charity who will not use the money ethically, as with the Trump Foundation scandal²³ and the Oxfam scandal²⁴. Lastly, the time risk relates to the time a potential donor would have to spend to make a donation. For example, donating blood takes more time than donating money to a charity, but less time than volunteering.

²³ <https://www.nytimes.com/2019/12/10/nyregion/trump-foundation-lawsuit-attorney-general.html>

²⁴ <https://www.theguardian.com/world/2018/feb/11/oxfam-staff-raise-concerns-over-charity-vetting-processes-haiti-abu>

These risks, even though they are here introduced in the context of the traditional types of donation, can be extrapolated and applied to the context of data donation. An individual may perceive physical risks, as is the case of, for example, an individual being afraid of being geo-located through the data donated thus putting themselves at risk. Social risks may be perceived if, for example, third parties have access to the individual's personal information and the individual perceives that that information may cause his social status to be negatively impacted. Psychological risks as, for example, having someone know everything about one's life can cause embarrassment for the individual as well as a feeling of vulnerability, thus impacting their mental state. Financial risks concern the risk of having one's financial data exposed and misused by third parties, including identity theft, fraud, and other financial crimes. Performance risks arise as a result of concerns about whether a charity may use donated data for anything else than for a specified and legitimate charitable purpose. Time risks arise if the data donation processes are too time consuming for an individual, particularly if they are not technologically literate.

Barkworth and colleagues (2002), mainly investigate the relationship between perceived risks and blood donation with focus on a donor's donation frequency. In their study, the authors surveyed a total of 206 blood donors across different venues while they were in the waiting room prior to the donation. The questionnaire was designed to assess the donor's sociodemographic characteristics, frequency of donation and perceived risk based on a specific set of categories: physical, social, psychological and time. These categories were adopted to the study of donation from Mitchel's (1999) work in consumer behaviour.

The authors found that the frequency of donation has a strong correlation with the physical and psychological perceived risks. In fact, individuals that did not donate for at least one year had higher physical and psychological perceived risks than those who donated at least once in the last twelve months. However, the results demonstrate that high trust levels in the Blood Transfusion Services reduce the perceived physical and time risks associated. Lastly, the authors concluded that the social risk is the most important of perceived risks. What if, along with the blood tests conducted in every blood donation, it would be found that the donor has HIV and this information would somehow spread across the donor's social circle?

Privacy is notably absent in their study and framework used, even though problematic information flow seems to feature in many of their harms. For instance, in the case of the social risk, the donor is afraid that damaging information about them may be found and that they cannot contain its spread. The same may happen in the case of data donation: when an individual donates their data, they may be incurring a risk that any analysis made to that data may uncover something potentially damaging to them.

Another shortcoming of this study is its focus on individuals who were ready to donate blood. This indicates that they had already made the decision to donate and considered all the possible risks. The fact that they did not consider the blood donation process to carry physical or time risks, does not indicate that the ones that considered and decided not to donate attribute the same importance to the risks. In a similar study, Nonis and colleagues (1996) investigate the existence of different perceived risks between donors and non-donors. The dimensions of perceived risk analysed are the same as Barkworth

and colleagues: psychological, social, physical and time risks. However, this study differs by taking in consideration non-donors instead of only donors, thus analysing which risks impact the most an experienced donor and a new donor.

Nonis et al. (1996) conducted a survey among 195 students from a large state university in the United States of America. Of the sample, 121 individuals donated blood at least once in the past, whereas only 76 never donated. Despite this, the authors found no difference in perceived risks between donors and non-donors. Furthermore, the authors claim that when blood banks try to minimise perceived risks by advertising the safety of the process, donors and potential donors are reminded of these risks and may re-consider their decision to donate.

Allen and Butler (1993) had already investigated the relationship between knowledge and perceived risk (psychological, social, physical and time risks) on the intention to donate blood. These authors surveyed a total of 430 individuals registered as blood donors, and found that, in contrast to their initial hypothesis, a higher donor knowledge about the process of blood donation does not reduce the perception of risk. In fact, the more an individual knows about the process the more risks they perceive. It was also found, as expected, that the individuals perceiving a higher level of risks in blood donation were less willing to donate. The three studies here reviewed achieve practically the same conclusions and all agree that a donation process always features at least one of these risks: social, psychological, physical, and time risks. The importance an individual attribute to each risk will influence their decision to donate.

Lastly, as previously exemplified, data donation has the potential to carry the exact same risks as the traditional types of donation.

Conclusively, where the trust in the blood bank / Blood and Transplant Centre (NHSBT) is high, perceived physical and time risks are diminished. Other complex types of donation, such as organ donation, carry the same perceived risks (Russel and Jacob, 1993; Alexander and Zola, 1996). While living organ donation carries physical (e.g., surgery), psychological (e.g. demanding process and testing), social (e.g. potential disapproval by family members) and time (i.e. time-consuming process) risks, posthumous organ / body donation only carries perceived psychological (it is not an easy decision) and social risks (e.g. where there may be a possible disagreement from family and close friends). Monetary and product donations are not as complex as organ or blood donations and, typically, only incur financial and performance (Iwaarden et al., 2009) perceived risks. Donating data, however, is a challenging process, especially for those who are not very involved with technologies. Therefore, when asked to donate their data, individuals who are not as tech savvy may be deterred by the time and proactiveness needed to gather their own data and give it to the charity. Those who are tech savvy and knowledgeable about the potential of contemporary technologies may be deterred due to their awareness of the potential risks associated with sharing their information, as demonstrated by Allen and Butler (1993).

Barkworth and colleagues' (2002) study, as well as many other donation studies (see Allen and Butler, 1993; Iwaarden et al., 2009) did not consider privacy as an added dimension that may have an impact in donors' behaviour. These studies omitted

privacy as a potential risk that may have been important for the participants studied. This research considers the privacy dimension because it is very relevant to data donation, and, thus, how individuals construct the risks of donating their data may be influenced by it. For example, an individual considering donating their personal data to a smart city may conceive that if their data is sold to their insurer, their cover and premium may be affected – in other words, they can argue a financial risk. However, because of the essence of what is donated (i.e. personal data) they may also argue privacy specific risks, as can be the case of their data getting sold, without their consent, to a third party. Here the individual may also argue that there is a risk that their data can be disseminated. Evidently there is a privacy dimension added to the traditional dimension of data donation. The question that warrants addressing is how this privacy risk dimension relates to the traditional risks explored by Barkworth and colleagues (ibid): how do they interplay in the way individuals construct the risk of donating their personal data?

Figure six below illustrates the risks experienced by individuals when consider whether to donate, as explored in this section.

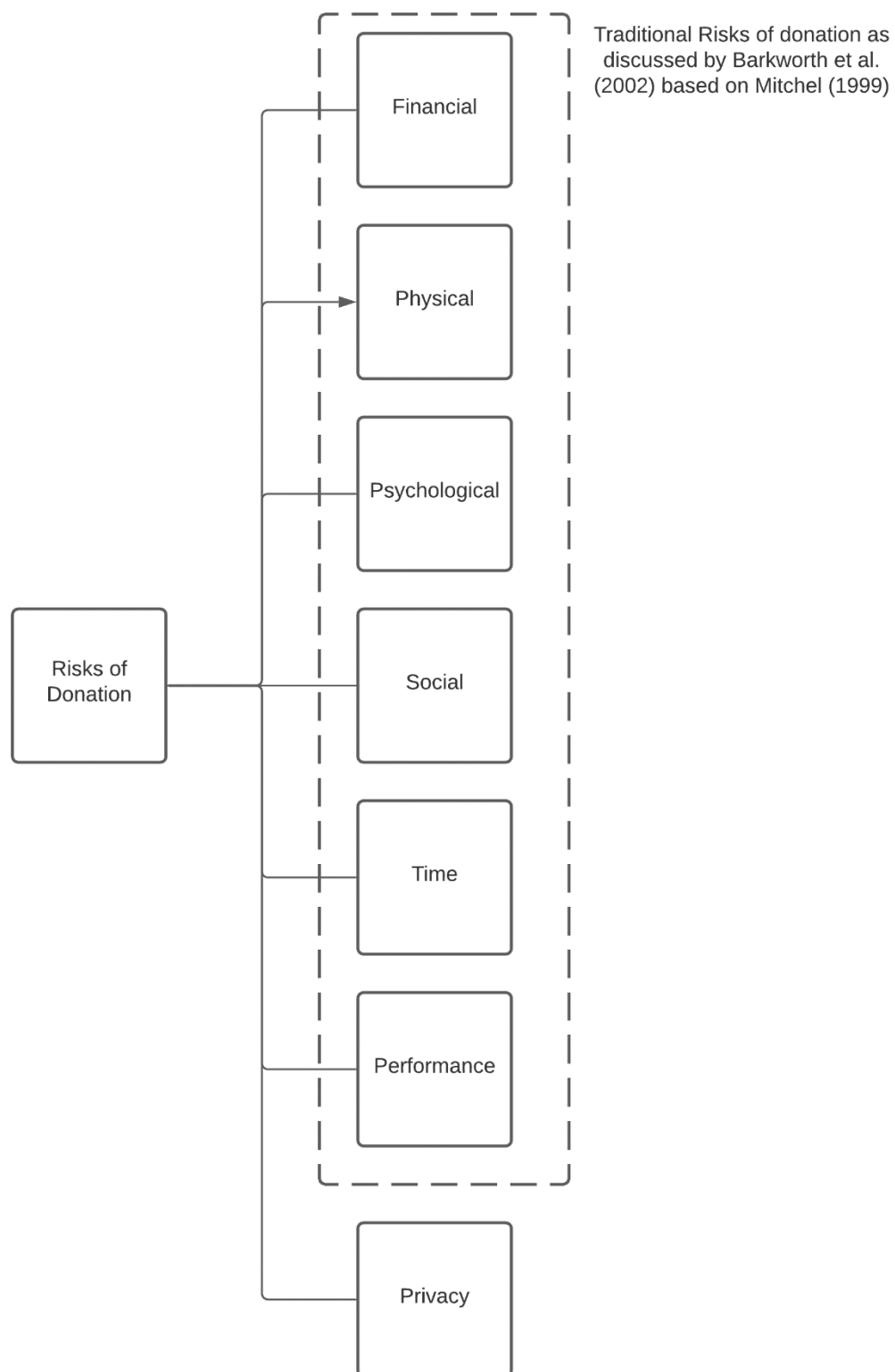


Figure 6 - Risks of Donation

Source: The Author

2.6 CONCLUSION

Donation plays a critical role in a country's economy and in the lives of the recipients. However, there is also an important impact in the lives of the donors that ought to be considered. Some things are easier to donate than others. Donating money, for instance, may be somewhat simple and straightforward (e.g., through gift aid or direct debit). In contrast, donating blood takes longer and generally requires more effort by the donor. Throughout this chapter, the most common types of donation were introduced, discussed and compared to the concept of data donation. A striking difference between the traditional types of donation and data donation is that, traditionally, once an asset is given, the beneficiary retains control or ownership of the donated asset. For instance, once £10 are donated, the donor's net worth decreases by that amount while the beneficiary's increases by that same amount. And the same is true with all the other traditional types of donation: blood, organs, products and time. Once someone volunteers for one hour in a food bank, that same person cannot get that time back, or that time cannot be used for anything else. In contrast, since data can be easily copied, even when given to a third party, the donor can still retain and have access to the data that was donated. Does this mean that when an individual gives their information to Facebook, for instance, is donating their personal data? What distinguishes data being shared from data being donated? This chapter has argued that for an action to be considered data donation, instead of data sharing, three criteria need to be fulfilled: 1) The donor should proactively acknowledge the transfer of personal data; 2) The data must be formally requested and not simply collected; 3) The recipient of the data should be acting and using the data for a wider social benefit. According to

these criteria, a first definition of data donation was proposed. After establishing the concept of data donation guiding this thesis, as well as introducing what makes it different from the traditional types of donation, the different motivations and experienced risks of donation were explored.

The way information flows regarding an act of donation is an issue thus far ignored by donation studies. This issue can be an important addition to the understanding of traditional forms of donation, along with being a central component of data donation and so it merits attention. Accordingly, privacy is now added as an extra layer being explored in the context of data donation. Namely, privacy implications associated with it and how privacy-specific risks may interplay with traditional donation risks. The next chapter explores how privacy risks may feature in acts of data donation and suggests and how they may be studied.

Chapter 3: EXPLORING PRIVACY

3.1 INTRODUCTION

The previous chapter introduced the concept of data donation, investigated and discussed the motivations and risks individuals may experience when deciding whether to donate a number of different types of assets, including data. However, even though faintly hinted by Barkworth and colleagues (2002), privacy, as an added dimension to the study of donation was not explored. In this study of data donation, privacy and its implications are considered as an extra layer influencing how individuals experience data donation and its risks. When donating data, an individual provides personal information about themselves to the recipient – effectively, that is what it is being donated. Data such as, for example, the individual's sociodemographic profile, online and offline purchase behaviour, their location history, amongst other things, can be donated, thus having privacy implications.

Accordingly, donating data can carry additional privacy risks to those initially discussed in the previous chapter. Although these privacy implications were hinted by Barkworth and colleagues, they were not explored and promptly dismissed. For instance, an individual that may discuss a social risk based on the fear that others may have access to certain information also carries a privacy-specific harm related with the disclosure of information. This chapter focuses on exploring these privacy-specific

risks, by first attempting to conceptualise privacy, establishing its importance for the individual and the society, and then continuing by discussing the potentially perceived privacy-specific risks of donating personal data.

This chapter addresses the different types of data that can be donated, attitude of individuals towards data donation, and how those risks can be experienced by them. It starts by discussing the fundamentals of privacy theory where the work of Westin (1967) and Clarke (1997) are discussed. These works enable the exploration of the different issues of data donation. For instance, that types of data that can be donated and different attitudes of donors towards the privacy implications of donation. However, as Westin and Clarke do not explore the social situatedness of data donation, the work of Irwin Altman is then discussed. With Altman's work a shift towards the social importance of privacy takes place.

In light of the argued paradigm shift from previous individual-centric conceptualisations of privacy to privacy as socially embedded, the chapter continues by discussing the social value of privacy focusing on the work of Steeves (2009), Regan (1995), and other colleagues. Specifically, it discusses the key role of privacy for individuation and relationship-making, as well as the importance privacy holds to a democratic and free society. From here, the chapter introduces Nissenbaum's (2010) theory of privacy as contextual integrity where the argument that privacy expectations are tied to the appropriate flow of information is discussed. With Nissenbaum's work this chapter explores the concept of felt risks and how individuals may experience different harms in different contexts, depending on the way their information flows.

After arguing for a conceptualisation of privacy as a social value, this chapter carries the idea of felt risk and examines Solove's (2006; 2008) privacy harms framework. Solove's work becomes essential as an a priori framework of reference to explore empirically how individuals think of the risks associated with data donation.

3.2 FUNDAMENTALS OF PRIVACY

This section introduces and discusses different conceptualisations of privacy and the potential privacy risks associated with donating personal data. As this thesis moves to understand the privacy implications of donating data, it is essential to understand what privacy and its importance for individuals and society is. However, defining privacy is no easy task. Philosophers, social scientists, legal scholars, amongst other scholars have attempted to come up with an acceptable definition, and so far, as is the case with most definitional debates, none have been met with consensus (Solove, 2008; Price and Cohen, 2019). Nonetheless, in order to be able to conduct an analysis of privacy and surrounding issues, it becomes essential to first conceptualise it and discuss the importance it holds for individuals and society.

Motivated by, in part, the increasingly intrusive attitude of newspapers²⁵, and the advance of new technologies, Warren and Brandeis (1890) authored the first article considering people's 'Right to Privacy', as it was entitled (Solove, 2006). Well over

²⁵ E.g., Bingham and Conboy, 2015: <https://reviews.history.ac.uk/review/1825>

one hundred years ago, the camera was the new technology that was considered a privacy danger. As Warren and Brandeis (1890) note, as photography became increasingly portable and inexpensive²⁶ and, thus, accessible to the general public, it became possible to take candid photographs unbeknownst to others. This technological advancement, combined with the increasingly intrusive attitude of the media posed a threat to people's "sacred precincts of private and domestic life" (Warren and Brandeis, 1890, pp. 195). Accordingly, in the first legal conceptualisation of privacy, Warren and Brandeis (1890, pp. 205), argue that individuals should have the "right to be let alone". From this argument, later on, privacy laws started being devised to protect people's right to privacy (Solove, 2006). From here, the chapter proceeds by introducing and discussing some of the most influential conceptualisations of privacy and how they evolved from being centred around the individual to being conceived as a social value.

3.2.1 WESTIN'S APPROACH

Westin (1967), in his seminal book 'Privacy and Freedom', argues that privacy relates to the manner in which individuals shield themselves and their information by temporarily and selectively limiting access to others. Privacy is here conceptualised as one's control over the access to the 'self'.

²⁶ In 1884, the Eastman Kodak Company introduced the 'snap camera'. A portable camera for the general public. Previously, cameras were expensive and of substantial size.

“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve.” (Westin, 1967, pp. 7)

Additionally, Westin argues that privacy is both a dynamic process, as individuals regulate the access to themselves according to different contexts and needs, and a non-monotonic process, as people can have too little privacy and too much privacy, as well as just the right amount of privacy. In fact, Westin postulates that privacy is a means to an end. In other words, individuals seek an ideal state of privacy in order to feel emotionally adjusted to their daily lives. Essentially, privacy is a regulatory mechanism that enables individuals to achieve happiness and balance in one’s life.

Westin (1967) proposes four ways in which the ‘ideal’ state of privacy can be achieved: solitude, intimacy, anonymity, and reserve. Solitude is the isolation of the self from others. Intimacy relates to close familiarity with another person or small group of people. Anonymity refers to the avoidance of identification in public contexts. And, reserve relates to the reluctance in disclosing certain information to others. These states seem firmly grounded on the fact that society is made of a series of individual entities (people, groups, and institutions) constantly looking for an ideal state of privacy, and, consequently, consciously controlling what kind of information

they disclose or keep private. If this were true, however, people would eventually become antisocial, isolated (Steeves, 2015), and their willingness to donate personal data would be challenged. Accordingly, in Westin's theory, the individual and the social are in constant state of tension as if rich social interactions prompted a deficit in privacy.

Westin's (1967) theory fails to admit that people are social beings, and, even if an individual seeks a more private state, and withdraws from wider social interactions, there will always be some degree of disclosure happening, especially with people closer to them. However, and although Westin (ibid) fails to admit the sociality of individuals, his theory presents limited notions of sociality. For example, Westin (1967, pp. 7) discusses "small group intimacy", thus admitting the importance of privacy being regulated not only at an individual level, but also at a group level. This will be further developed in section three of this chapter.

Westin tried to understand how individuals reacted to privacy differently. For this, Westin (2000), advanced the Privacy Segmentation Index. In this index, Westin suggests that individuals can be privacy fundamentalists, pragmatists, or unconcerned (Kumaraguru and Cranor, 2005). In theory, as fundamentalists are more suspicious to any request that might endanger their privacy, they are often opposed to disclosing any type of personal information. Pragmatists carefully consider the potential risks of giving their information and weigh them against possible rewards. Unconcerned individuals are willing and at ease with disclosing their personal information, as long as they believe the information is generally safe (Elueze and Quan-Haase, 2018).

When considering these Westin's categories, it is possible to apply these attitudes in the context of data donation. For instance, fundamentalists may not be interested in donating their personal data as they are increasingly concerned about it how it may be used. Pragmatists will consider the potential positive and negative implications of donating their personal data, taking a more careful, almost as if rational, approach. Lastly, unconcerned individuals will quickly dismiss any potential risks, taking a more relaxed approach towards data donation.

Woodruff and colleagues (2014), criticised this index, arguing that previous research has failed to link these three categories, to privacy-related behaviours and attitudes (e.g., Jai and King, 2016; Jensen, Potts, and Jensen, 2005). The authors investigated whether these generic privacy attitudes are linked to actual attitudes and behavioural intentions when individuals face potential consequences of protecting or disclosing their personal data online. To do so, they surveyed 884 Amazon Mechanical Turk participants, an online platform that allows institutions to advertise small tasks better suited to a human to perform in exchange for cash (e.g., surveys). Various scenarios and consequences were presented, but all involved participants trading off a benefit (e.g., \$1000, potential discovery of a cure for a disease) for a cost to their privacy (e.g., sharing their personal data, anonymised or not, with a third-party, that may publicly disclose it).

In theory, Westin's categories are designed to help predict individuals' behavioural intentions towards each scenario. However, Woodruff and colleagues (2014) found no relationship between these categories and the attitudes and behavioural intentions of

participants. They found, for example, that a privacy fundamentalist would be willing to sell their DNA for \$1000. This contradicts what Westin postulated. As mentioned, similar results were observed in other studies (e.g., Jai and King, 2016; Jensen et al., 2005). The authors suggest that this lack of correlation, and, therefore, lack of the predictive power of Westin's Index, may be due to the fact that an individual's behaviour is "based on a context-sensitive cost-benefit analysis, mediated by complex factors, such as systemic biases in decision-making, that are not captured by generic broad privacy attitudes" (Woodruff et al., 2014, pp. 12)²⁷. In fact, when there is uncertainty expressed about an individual's privacy preferences, context plays an important role. Therefore, as contexts often changes, individuals can exhibit different attitudes to privacy, ranging from extreme concern to apathy: "Adopting the terminology of Westin, we are all privacy pragmatists, fundamentalists, or unconcerned depending on time and place" (Acquisti et al., 2015, pp. 511). Accordingly, the context in which data donation occurs, and the conditions mediating it will influence how individuals respond, the risks they perceive, amongst other things.

Elueze and Quan-Haase (2018), based on their empirical test of Westin's categories in older adults (65+ years old), proposed an updated version of Westin's segmentation: fundamentalist, intense pragmatist, relaxed pragmatists, marginally concerned, and cynical expert. The authors argue that intense pragmatists, similarly to fundamentalists, are private individuals, unwilling to disclose personal information,

²⁷ These can both be perceptual and behaviour biases

however, in some specific contexts, understand the necessity to disclose private information. For example, an intense pragmatist may not be willing to disclose information to Facebook, however, they may be willing to donate their personal data if that means lives can be saved (e.g., donating data to contact tracing apps). Furthermore, relaxed pragmatists, even though concerned about the risks of disclosing information, expressed fewer concerns than intense pragmatists. The marginally concerned expressed almost no concerns regarding the disclosure of private information. Lastly, the cynical expert, refers to those who express a high degree of scepticism about sharing or donating personal data online due to mediatised forms of surveillance. For instance, in Elueze and Quan-Haase's (2018) study, one participant reported being afraid to engage in activities online due to possible NSA surveillance as made public by Edward Snowden.

In order to reach this categorisation, the authors interviewed 40 individuals in East York, Canada, aged between 65 and 91 years old, with a mean age of 73.4 years old. This demographic was previously thought to be very concerned about their online privacy (fundamentalists), resulting in limited social media use. However, their findings were rejected (i.e., the majority of the respondents were not found to be fundamentalists), and some support for Westin's categories was found, leading to the proposal of the updated segmentation categories. It is, nonetheless, important to note that context is very important, so it is expected that different studies in different contexts will yield different outcomes. Lastly, the sample size used in their study is regarded as insufficient for a typical segmentation study (Dolnicar et al., 2014; Dolnicar, Grun and Leisch, 2016). Accordingly, if Eluaze and Quan-Haase's (ibid)

and Westin's work can be criticised due to a degree of context specificity, then the context in which data donation occurs may raise specific privacy concerns. This issue will be picked up further in section 3.4. The chapter continues by discussing Roger Clarke's conceptualisation of privacy, that is in many ways similar to Westin's, but it differs by moving past the reductionist definition of privacy as a form of control of access to the self.

3.2.2 CLARKE'S APPROACH

Roger Clarke's (1997) approach to conceptualising privacy is similar to Westin's in that it is a categorical approach. However, it differs by attempting to move past the conceptualisation of privacy as a form of control of access to the self. Instead, Clarke (1997) introduces different dimensions of privacy: privacy of the person, privacy of personal data, privacy of personal behaviour, and privacy of personal communication. Equally, in the context of this research, these may represent different types of data that can be donated. Privacy of the person is related to the integrity of a person's body and its functions (e.g., medical treatments, samples of bodily fluids, biometric measurements). Privacy of personal data is connected with data protection issues and the misappropriation of one's data. Privacy of personal behaviour refers to one's personal behaviour and attitudes, such as religious, sexual, and political practices. Particularly, it refers to the rights people have to a private space in order to carry these and other practices free from any kind of surveillance. Lastly, privacy of personal communication refers to the rights one has to communicate freely, either via electronic means or face-to-face, without being subject to surveillance. This last social need

builds on Westin's notion of an individual's control of what others know about them. Accordingly, instead of a conceptualisation of privacy focused on individual perceptions, Clarke advances a categorisation of privacy needs, or, in other words, a categorisation of what individuals value. As a justification for his 'privacy-values' conceptualisation, he argued: "interpreted most broadly, privacy is about the integrity of the individual. It therefore encompasses all aspects of the individual's social needs" (Clarke, 2006).

Finn, Wright, and Friedewald (2013) expanded Clarke's taxonomy from four categories to seven, arguing that exponential technological advances meant that the earlier categorisation was no longer comprehensive enough to expose the wealth of potential privacy invasions (e.g., the use of drones, body scanners, and RFID technologies). The updated taxonomy includes privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy). Similar to Clarke's work, all these represent categories of information that can be donated. Finn and colleagues' (2013) updated classification builds on Clarke's (1997) in order to provide a more comprehensive framework, that is mindful of the contemporary state of technology. As an example, the growth of surveillance technologies enabled platforms to not only observe people's online behaviours (i.e., what they see and how they interact with their page), but also what actions do they perform in and out of their page. For example, a company using

‘cookies’ to be able to track people’s journey throughout the internet²⁸. Consequently, it is vital to understand the necessity to protect not only people’s behaviours, but also their online and offline actions.

Finn and colleagues (2013), as with Clarke (1997), refer to the privacy of the person as the right of keeping the aspects and characteristics of the human body, and everything that makes it uniquely identifiable (e.g., biometric data) private. Privacy of behaviour and action refers to any type of information that may inform on an individual’s lifestyle (e.g., sexuality, religion, political beliefs, sexual habits). However, this behaviour can be argued to be either private or public, as there may be casual observation by people in a public space (e.g., someone watching a homosexual couple kissing). Nonetheless, the issue addressed by this category is the capability to act and behave in a private or public space without being monitored and its information stored and used by third parties. Privacy of communication encompasses the right to freely communicate with others without being subject to surveillance (e.g. the use of covert listening devices, monitoring of emails). This type of privacy is addressed by many governments by requiring a legal warrant before any surveillance takes place.

Privacy of data and image refers to an individual’s data (e.g. online metadata, social media pictures), and their right to have that data protected and inaccessible to others. In addition, this type of privacy encompasses the right people have to exert control over their data and how it can be used. Consequently, “this aspect of privacy has social

²⁸ <https://www.consumer.ftc.gov/articles/0042-online-tracking>

value in that it addresses the balance of power between the state and the person” (Finn et al., 2013, pp. 5). This happens by allowing the individual to remain in control of the data they generate, and choose who, how, and when can use that data. Totalitarian regimes are infamous for their need to control the society, especially, what they say about who is in power. In this regime, an individual’s right to choose who, when and to which purpose, has access to their data is severely limited, thus, the power is with the state and not with the individual. Furthermore, unrestricted surveillance has a profound impact on political discourse by limiting people and groups’ ability to express their political opinion through peaceful protests. Therefore, balancing the power between the state and the person, and limiting what a state can possibly know about an individual, allows not only to protect people’s autonomy, as well as it ensures enough freedom to exercise other fundamental rights (Goold, 2009).

Privacy of location and space refers to the right one has to move in public or private spaces without being monitored. This type of privacy, as with privacy of data and image, features as a social value: when individuals are free from surveillance and can freely move both in private or public, they experience a higher sense of democracy and freedom. This is due to the fact that they can practice their ideologies and beliefs, as part of social groups (e.g., taking part in a public demonstration) without being surveilled (Finn et al., 2013).

Privacy of association refers to the right one has to associate with anyone without being subject to surveillance (e.g., political parties). As with the previous categories, this privacy of association also features a social value. Individuals ought to be free to

gather in groups, ideological or not, and carry out their lives as such without the subjects, and, in consequence, the group, being subject to surveillance.

Lastly, privacy of thoughts and feelings derives from Warren and Brandeis' (1890) argument that privacy not only relates to physical intrusions in one's daily life, but also to the harm done to one's feelings. This way it is just as important to protect the privacy of individuals' thoughts and feelings in an increasingly technologically invasive society.

This expansion of the Clarke's initial categorisation offers a more comprehensive taxonomy of privacy. It also allows for an understanding of the types of data that can be donated. For example, biometric data (privacy of the person), religious beliefs (privacy of behaviour), e-mail data (privacy of communication), social media data and pictures (privacy of data and image), itinerary data (privacy of location), political affiliation data (privacy of association), data pertaining to one's mood (privacy of thoughts and feelings).

The table below summarises some of the different categorical approaches to conceptualise privacy discussed during this subsection:

	Authors	Proposal
States of Privacy	Westin (1967)	Solitude; Intimacy; Anonymity; Reserve
Types of Privacy / Categories of Data That Can Be Donated	Clarke (1997)	Person; Data; Behaviour; Communication
	Finn et al. (2013)	Person; Data; Behaviour and Action; Communication; Data and Image; Thoughts and Feelings; Location and Space; Association
Segmentations / Attitudes Towards Data Donation	Westin (1995): Privacy Segmentation Index	Fundamentalist; Pragmatist; Unconcerned
	Eluaze and Quan-Haase (2018)	Fundamentalist; Intense Pragmatist; Relaxed Pragmatist; Marginally Concerned; Cynical Expert

Table 2 - Categorical Approaches to Conceptualise Privacy

The body of work so far discussed sets out what might be donated (i.e., type of data as per Clarke's and Finn and colleagues' work), the kind of attitudes people may have towards donating their data (i.e., Westin's and Eluaze and Quan-Haase's work), but it does not delve into the social situatedness of that act of donation. Although Westin

hints at the importance the social has to an ideal privacy state (i.e., the tension between social and self), his work does not investigate it. The following section, and the work that follows, introduces the social value that privacy holds to the understanding of the risks involved in donating personal data. Furthermore, it explores how individuals can be concerned with their personal boundaries when donating personal data.

3.2.3 ALTMAN AND THE PRIVACY REGULATION THEORY

Irwin Altman was an environmental psychologist with a keen interest in privacy and territoriality. As with Westin, Altman argues that privacy is “the selective control of access to the self” (Altman, 1975, pp. 24). Equally, Altman also places privacy at the heart of complex social interactions, where he argues that individuals and groups seek a balance between being open and closed to interactions. Altman, however, diverges from Westin in the way individuals seek to achieve their ideal level of privacy. Although they share the idea that people actively pursue a balance between their level of openness and closeness, Altman disagrees with Westin’s ‘social withdrawal’ argument. Accordingly, privacy becomes a dynamic process of negotiation between being open and closed. Altman (1975, pp. 6) defines privacy as:

“An interpersonal boundary process by which a person or a group regulates interaction with others. By altering the degree of openness of the self to others, a hypothetical personal boundary is more or less receptive to social interaction with others. Privacy is, therefore, a dynamic process involving selective control over a self-boundary, either by an individual or a group.”

Altman (1975) proposes five properties of privacy: privacy is a dynamic process of social boundary control as an individual changes their level of openness and the levels of disclosure depending on their privacy needs. Therefore, as with Westin, a distinction is made between actual and desired privacy levels. In accordance with Westin, an individual can have too much, too little, and ideal levels of privacy. Additionally, privacy is bi-directional as it involves inputs and outputs from third parties. Lastly, privacy is not only an issue of an individual but can be also applied at a group level (Altman, 1975, Margulis, 2003).

Accordingly, privacy is no longer conceptualised as an individual's control over the flow of their information, as previously postulated, but as a result of "an interpersonal event, involving relationships among people" (Altman, 1975, pp. 22). When, for example, private information is disclosed to others, individuals become "co-owners" of such information. This co-ownership encompasses an expected degree of responsibility to protect and maintain the information private. Therefore, when disclosing information, individuals expect this to be shared and protected according to implicit, or explicit, norms. Moreover, according to Altman, privacy is regulated by controlling the access to their private information with inputs (e.g., controlling who enters one's house), and outputs (e.g. controlling what is disclosed to others), in order to achieve a desired level of privacy. Consequently, privacy has three goals: the regulation of personal boundaries; the development and management of interpersonal relationships; self-observation and self-identity (Altman, 1975, pp. 47-48). These are tied to an individual's identity and how they come to experience subjectivity. Therefore, and as long as individuals can control "what is me" and "what is not me",

then they can comprehend who and what they are (Altman, 1975, pp. 50; Steeves, 2009, pp. 202). When donating personal data, individuals may be concerned with maintaining their personal boundaries. According to the type of data being donated, its intended use, and the closeness of the relationship between the donor and the recipient, individuals will try to negotiate their boundaries.

Privacy and identity are concepts embroiled in one another. Fundamentally, privacy becomes an essential part of the self. Thus, the integration of one's experiences and social interactions allows an individual to exercise their autonomy and self-determination. Individuals compare themselves with others from a same social group (in-group) or other social groups (out-group) and this helps them understand who they are and how others see them. It is a fundamental process of an individual's identity formation (i.e., individuation) (Hogg, 2000). Privacy, therefore, is the mechanism that aids the regulation of individuation – In Altman's (1975, pp. 47) words:

We use other people to help label our feelings and define our perceptions. It might be said, therefore, that one function of privacy is to assist in the social-comparison process – at the interface of the self and others. As such, privacy regulation may enable the person to decide on courses of action, to apply meanings to various interpersonal events, and to build a set of norms or standards for interpreting self/other relations.

Around the same time that Altman discussed this conceptualisation of privacy, he was also, in collaboration with Taylor, developing the Social Penetration Theory, that, to some extent relates to his conceptualisation of privacy. The Social Penetration Theory (Altman and Taylor, 1973; Taylor, 1968; Taylor and Altman, 1975) was developed in order to provide an explanation of how interpersonal relations evolved. In simple terms, how do humans go from strangers, to acquaintances, to friends. The theory is based upon the premise that as individuals gradually disclose more intimate information about themselves to one another over time, their relationship will change, becoming deeper.

Altman, however, was an environmental psychologist, and, according to Margulis (2003), he was mainly interested in the relationship between human social behaviour and the physical environment. Therefore, his work on privacy derives from the observation of the relationship between territorial behaviour and the private space. In fact, Altman postulates that a person's environment is a key element to the boundary negotiation process. Specifically, Altman posits that environmental elements, such as an individual's personal space, clothing, and territoriality, constructs the three environmental mechanisms of privacy (Altman, 1975, Archea, 1977, Margulis, 2003). He argues that these mechanisms are not only a determinant but also an extension of an individual's privacy behaviour. By combining inputs and outputs with different environmental mechanisms (e.g., physical environment, territorial behaviour, cultural norms) individuals are able to regulate their privacy (Margulis, 2003).

Altman's and Westin's theories are examples of a limited-access conceptualisations of privacy in that both focus on the importance of regulating or controlling the access to the self, respectively. Equally, both theories look at privacy at individual and group levels. Both are relatively narrow approaches to privacy in that they contend that individuals open or close themselves to social interactions according to their current privacy status with the goal of achieving an ideal level of privacy. Nonetheless, Altman's, and, to a much lesser extent Westin's, works are rich in sociality. They feature privacy as being of social importance, however, often, this is an implicit theme rather than fully drawn out in their contributions. The next sections will discuss precisely that: The social value of privacy, and how it is at the epicentre of relationship-making, individuation, and essential to a democratic and free society.

3.3 PRIVACY AS A SOCIAL VALUE

3.3.1 COMMUNICATION PRIVACY MANAGEMENT AND THE FOCUS ON RELATIONSHIPS

Throughout the last sections I explored several theories that look at privacy as being crucial for the individual. However, with Altman's work one can already observe that privacy may play a larger role than simply being individual-focused. Petronio (2002), places privacy as essential for human social interactions. Especially, she focuses on privacy as fundamental to the development of relationships. In her Communication

Privacy Management Theory (CPM), Petronio (2002, pp. 3), suggests ways “privacy boundaries are coordinated between and among individuals” and allows for an understanding of the tension inherent to deciding whether or not to disclose private information. As hinted by the quote, CPM is rooted in Altman’s (1975) work. In fact, Petronio (2004) even acknowledges that, while little information was available to understand the concept of disclosure, Altman and Taylor’s (1973) Social Penetration Theory (SPT) offered useful insights. Although the SPT, as briefly discussed earlier in this chapter, primarily concentrates on the development of relationships, the authors discuss notions of self-disclosure as the cornerstone of relationship-building dynamics. Data donation, the focus of this thesis, as with other types of donation, in its most simple form, ends up being an interaction between individuals, thus mobilising Altman’s and Petronio’s work.

CPM is supported by three main principles that guide individuals’ privacy choices. First, individuals assume they have ownership of their private information. This belief, helps them perceive boundaries, thus allowing them to grant, or not, others access. This perceived control over their own information leads to the second principle: privacy regulation. This contends that individuals set up their own privacy rules as a way to regulate the flow of their private information. In consequence, if an individual discloses their information to others, they expect the third parties, that now became co-owners of said information, abide by the original owner’s rules: “original owners see the recipient having fiduciary responsibilities for the disclosed information” (Thompson, Petronio and Braithwaite, 2012, pp.57). The last principle refers to the phenomenon that occurs when recipients of private information do not know or

conform to the privacy rules expected by the owner. This phenomenon is denominated of privacy turbulence or breakdown in the privacy management system (Petronio, 2002, 2010; Thompson, Petronio and Braithwaite, 2012).

CPM was used in a plethora of works delving into how individuals choose to disclose information, how co-owners regulate jointly agreed privacy rules, among other things. For example, Thompson, Petronio and Braithwaite (2012, pp. 54), employed the CPM in order to examine “privacy rules for academic advisors and college student-athletes”. As advisors and students have an intimate relationship, where students often disclose personal information (e.g., mental health struggles), the researchers (ibid, pp.54) sought to understand how advisors determine privacy rules used to disclose or not the private information revealed by their student. In different studies, Waters and Ackerman (2011), used CPM in order to explore the different motivations and perceived consequences of disclosing personal information on Facebook, and Brummet and Steuber (2015) to understand the privacy management process among interracial couples.

Through this lens, one can argue that privacy has social value embedded in its core. Privacy and the associated boundaries and regulations are at the centre of the phenomenon that eventually enables the development of relationships between individuals (e.g., advisor and student), between an individual and a social group (e.g., Facebook user and audience), or between groups (e.g., interracial couple and parents) to evolve. Accordingly, it is equally possible that privacy – and its boundary negotiations – as an added layer to data donation, may be responsible for the

individuals' relationship with the institution to which they are donating their data to evolve.

Petronio and Altman's work help explore concerns individuals may have regarding their personal boundaries when donating personal data. However, as examined below, privacy can also play an important role in preserving an individual's identity and autonomy. Regan and Steeves' work help explore the social value of privacy, and how individuals may be concerned with preserving their identity and autonomy when donating their personal data.

3.3.2 PRIVACY AT THE EPICENTRE OF INDIVIDUATION AND RELATIONSHIP MAKING

Regan (1995), in her seminal book 'Legislating Privacy: Technology, Social Values, and Public Policy', argued that privacy is not only important to individuals but also to society. Besides arguing that individuals have common perceptions of privacy, Regan (1995) argued that privacy was equally important to the democratic process. Regan (1995, pp. 227) claimed that "the privacy issues raised by direct-mail marketing and by the targeting of political messages take on new significance – a more public significance [...]. One could argue that the privacy invasions that occur in the targeting of political messages violate the integrity of the electoral process [...]". Although this has always been of importance, fast-forwarding to the 2016 U.S. Presidential Elections, and the 'Brexit Referendum', Regan's words could almost be taken as acted as a prophesy. Furthermore, Regan argues that privacy is essential to the development

of individuals. Based on the works of Mill (1859), and Gavinson (1980), Regan (1995, pp. 222) maintains that “privacy is important, [...], because it enables the development of the type of individual that forms the basis of a certain type of society”. In essence, it is privacy that enables individuals to develop as unique and different from one another. This diversity is an integral part of the social fabric. Valerie Steeves (2009), amongst other authors, strengthened the argument of the social value of privacy, especially, the importance of privacy for an individual’s identity formation process (individuation). This way, and in the context of this research, individuals may be concerned about protecting their identity, and their autonomy.

Valerie Steeves builds on Westin, Altman and Mead’s theories reclaiming “the social value of privacy by focusing on the social interactions individuals undertake to negotiate the personal boundaries in their relationships” (Regan, 2015, pp. 57). However, while Steeves and colleagues discuss the value of privacy for the functioning of society, their focus is in studying the development of the self, where privacy plays a central role. For example, authors such as Regan, Steeves, Bailey, Burkell, among others highlight the importance and the role that privacy plays in self-development, especially in young people (e.g., Regan and Steeves, 2010; Bailey et al., 2013; Livingstone 2005, 2008; Cohen, 2012).

Steeves (2009, pp. 204) builds on Westin and Altman’s theories of privacy, and on George Mead’s work into the development of the self through communication in an attempt to frame privacy as a social value. In conceptualising privacy as a social value, privacy evolves from being, theoretically, important only to the individual and

becomes key to a functioning society and social interactions. Accordingly, the argument that policies should focus on protecting the individual's right to privacy, as, for example, the selective access to the self, augmented by notions of the social. In essence, the importance of individual preferences regarding privacy is minimised in favour of the social. This way, "privacy is worth taking seriously because it is among the rights, duties or values of any morally legitimate social and political system" (Nissenbaum, 2010, pp. 66).

Mead (1934) argues that the social development of the self is closely related to the development of language: people become aware of themselves as individuals as a consequence of continuous social interaction with others. These social interactions are made possible by the use of language: "the critical importance of language in the development of human experience lies in the fact that the stimulus is one that can react upon the speaking individual as it reacts upon the other" (Mead, 1934, pp. 69). This notion of the social self demonstrates a lack of friction between the individual and the social. Instead, the social is a precondition to the development of the individual's identity and personality. In consequence, "the tension between the social and the individual – which is so problematic in Westin's theory – dissolves" (Steeves, 2009, pp. 204). Steeves (ibid) claims that if the development of a person's identity derives from the awareness of the other and the self, privacy, framed as the barrier between the two, is, accordingly, situated at the centre of identity: "Privacy cannot, therefore, shelter the liberal ego from social interaction, as Westin posits; rather, privacy – as the line between self and others – is intersubjectively constituted through communication" (Steeves, 2009, pp. 205).

Furthermore, Mead (1934) claims that the development of an individual requires an engagement and participation in different social roles (e.g., Partner / Doctoral Student / Son). In accordance, due to the fact that these roles are essentially embedded in an individual's life, privacy is fundamental because it allows individuals to delineate boundaries between roles (Steeves, 2009). Essentially, it is privacy that allows a person to carry out a role (e.g., Partner) independently from another role (e.g., doctoral student). In line with this, interfering with one's privacy (e.g., through surveillance practices) is detrimental to an individual's life as it destroys the boundaries between their social roles, and makes them responsible for their actions, despite context.

Moreover, the tenet behind social identity (see Tajfel, 1979) may also help explain how individuals may act as part of a social group (e.g., cyclist, supporter of a particular football club, citizen of a particular city). One's social identity indicates who they are by understanding the groups to which they belong to, thus helping to predict certain behaviours. Reicher, Spears, and Haslam (2010) claim that when taking a social identity stance, we see people in terms of their group affiliation (e.g., their nationality, ethnicity), thus also giving space to stereotyping. These perceived group memberships have a significant impact in how individuals behave, including their pro-social behaviour. As found by Levine, Prosser, Evans, and Reicher (2005) individuals' group membership help determine their helping behaviour.

Accordingly, privacy plays an important role in protecting one's personal and social identity and autonomy. Therefore, when donating personal data, individuals may be concerned with protecting their identity and autonomy, that can be put in danger

should their autonomy be compromised. Helen Nissenbaum strengthens this argument placing privacy as being contextual, and dependent on the way information flows. The section below introduces and explores the idea that individuals may be concerned about the context in which their personal data is being donated and used should this be done beyond what they initially consented to.

3.4 CONTEXTUAL INTEGRITY

The social value of privacy was discussed throughout section 3.3. It was argued that privacy, as the epicentre for individuation and relationship-making, is essential to the development of the individual and to a functioning society. Privacy, amongst other things, is what allows individuals to perform different social roles. As social roles occur in different contexts it is likely that the risks associated with data donation may differ according to the context in which it takes place. For example, was the data donated pertaining to an individual's commute (i.e., individual performing the social role of a worker) or did they just go for a shopping trip? Without the opportunity to explain and contextualise personal data, one's actions and behaviours, both at an individual and group level, while on a given social role can be judged out of context. Accordingly, how individuals discuss the risks of donating their personal data can be tied to the context in which they are asked to donate their data: what is contextually appropriate to donate, between whom, and what informational norms govern this donation. This section discusses the role of privacy as contextual integrity, a concept proposed by Helen Nissenbaum (2004).

Nissenbaum's privacy as contextual integrity is not meant to be an attempt to define privacy. Instead, "is a philosophical account of privacy in terms of the transfer of personal information" (Barth et al., 2006). In Nissenbaum's work, privacy has a distinct social value in that it "serves to maintain different social contexts and the values of these different contexts" (Regan, 2015, pp. 59). In her theory of Contextual Integrity, Nissenbaum (2004, pp.119), argues that there is no element of human lives that is "not governed by [context-specific] norms of information flow". Religious, moral, cultural, among other norms influence the way individuals behave and act on their daily lives. Accordingly, people's behaviour is guided by these sets of norms. For example, where in some cultures individuals easily talk about their salaries, in others the disclosure of this information is restricted to a person's family (Barkhuus, 2012).

To Nissenbaum (2004), the notion of universal privacy norms is disregarded in favour of a more contextualised conceptualisation. In other words, a 'one-size-fits-all' conceptualisation of privacy, as discussed thus far, is, therefore, rejected in light of a flexible theory where the norms regulating privacy are adapted to different contexts. In this way, the duality of privacy thought as either limited access to information or control of personal information is avoided. In fact, Nissenbaum (2010, pp.147-148) recognises that "the framework of contextual integrity reveals why we do not need to choose between them; instead, it recognises a place for each". It is all dependent on the norms regulating a given context. For example, an individual is expected to be comfortable with sharing sensitive medical information with their doctor but not with their employer. In this case, there is a selective control of the access to one's personal information, however, it is context specific.

Accordingly, Nissenbaum (2010) proposes four key parameters to conceptualise context-relative information norms: *contexts* refer to the situations in which the transfer of information occurs (e.g. medical consultation); *actors* refer to the parties involved in the flow of information: who sends the information (e.g. patient), who is the recipient (e.g. doctor), and who is the information about (information subject); *attributes* refer to the types of data being transferred (e.g. demographic and medical data); *transmission principles* refer to the constraints to the flow of information from one actor to the other in a given context (e.g. medical consultation is guided by a set of transmission principles – the doctor ought not to disclose the information, amongst other norms).

Nonetheless, one of the critiques to the Contextual Integrity framework is that it is too conservative in tackling the challenges of new technologies (see Rule, 2019; Benthall et al., 2017). In consequence, it becomes increasingly hard to evaluate online informational norms. In response to this critique, Nissenbaum (ibid, 148) proposed a decision heuristic that serves for “determining, detecting, or recognising when a violation has occurred”. This decision heuristic is depicted below.

1. Describe the new practice in terms of information flows.
2. Identify the prevailing concept (e.g., Health care) and identify potential impacts from contexts nested within it (e.g., teaching hospital).
3. Identify information subjects, senders, and recipients.
4. Identify transmission principles.
5. Locate applicable entrenched informational norms and identify significant points of departure.
6. Prima facie assessment. A breach of information norms yields a prima facie judgment that contextual integrity has been violated because presumption favours the entrenched practice.
7. Evaluation I: Consider moral and political factors affected by the practice in question. What might be the harms, the threats to autonomy and freedom? What might be the effects on power structures, implications for justice, fairness, equality, social hierarchy, democracy, and so on? Evaluation II: Ask how the system or practices directly impinge on values, goals and ends of the context. What do harms, or threats to autonomy and freedom, or perturbations in power structures and justice mean in relation to this context?
8. On the basis of these findings, contextual integrity recommends in favour of or against systems or practices under study.

Table 3 - Nissenbaum's Decision Heuristic Table

Source: Adapted from Nissenbaum (2010, pp. 182)

Huang and Bashir (2015) apply the Contextual Integrity framework in order to investigate information flows in direct-to-consumer genetic testing. By examining the companies' privacy policy, presumed consent and terms of service, they investigated three distinct scenarios of information flow: users participating in a company's managed online community, consumers purchasing a genetic testing kit, and consumer participating in a given research. In the first scenario, users were posting and engaging with different individuals (consumers and company staff). They ask questions and

share personal information, such as ethnicity and possible illnesses, and then, the company, through the platform, processes such information and, among other things, displays it to the community. In the second context, the consumer orders a genetic testing kit, follows the collection procedure, and then the company's laboratory is responsible for the testing, sending back the results within a specific time frame. In the last scenario, consumers participate in research projects promoted or conducted by the genetic testing company. Users send their genetic samples to the company and then they pass it on to the researchers in charge.

Altogether, Huang and Bashir (2015), supported by the Contextual Integrity framework, look at how information flows in these contexts and discuss how an individual's privacy can be violated. In the first scenario, an individual's privacy may be violated when a third-party (e.g., other user, third party institution) collects one's personal, identifiable data. For example, the user's employer finds his online profile with disclosed medical data. In the second scenario, the uncertainty surrounding the ownership of one's genetic data may be damaging for the individual's privacy. Lastly, regarding the last context, some companies do not give an option for the consumer to withdraw their consent for the use of their genetic information for research purposes. The ever-present conflict between user's privacy and companies' profits is evident in the contemporary socio-technical climate. Although consumers are frequently seduced by claims of the use of genetic data for the greater good (i.e., mapping diseases and finding cures for deadly diseases), they are often concerned with their privacy, and the security of the institution collecting and processing their data (Hayden, 2013; Huang and Bashir, 2015).

Despite appealing to an individual's 'altruistic' self, companies use a plethora of promotional messages embedded in their business model in order to collect users' information. Take Facebook's mission statement, for example, "Give people the power to build community and bring the world closer together", or Google's mission "to organise the world's information and make it universally accessible and useful". Both these companies have, largely, free products and services used by billions of people. Undoubtedly, these products and services address people's needs to some degree (e.g., Facebook connects people and helps them keep in contact – "brings the world together"). Therefore, individuals [un]knowingly trade their personal information, monetised by the platform, in exchange for the fulfilment of that certain need. Nonetheless, despite this, whenever an individual decides to disclose their personal information, there may be specific privacy-specific risks that are understood by individuals (e.g., Van Zoonen, 2016; Zhou, 2017) that, as argued, are context dependent. Accordingly, privacy is understood as something which has numerous social dimensions within and between contexts.

Until this point, the different types of data that may be donated (Finn and colleagues, 2013; Clarke, 1997), and the different attitudes towards data donation (Westin, Eluaze and Quan-Haase, 2018) were discussed. Furthermore, it was also explored how individuals may be concerned about protecting their boundaries while donating data (Altman, 1975; Petronio, 2002; 2010), how individuals may be concerned about preserving their identity and their autonomy (Steeves, 2009; Regan, 1995; 2015), and, lastly, how individuals may have different concerns regarding data donation

depending on the context in which it takes place (Nissenbaum, 2010). However, how these risks are experienced, felt, and expressed by people remains unclear. Whilst the collection and processing of personal data increases the potential for harm, most of the damage to the individuals comes from the vulnerability associated with donating data. In other words, mostly, the harm is derived from the anxiety generated by the felt risk (i.e., vulnerability) rather than the risk itself (Martin, et al., 2017). The next section introduces and explores Solove's work into privacy-specific harms as this provides a suitable platform to explore these different dimensions of vulnerability, as well as how the risks are expressed by individuals.

3.5 PRIVACY-SPECIFIC RISKS

A potential donor's way to recognise risk encompasses two major factors: the possibility of an unwanted consequence from the donation and the existence of uncertainty in the occurrence of that consequence (Barkworth et al., 2010). As previously argued, data donation differs significantly from the other traditional types of donation, largely because of the unique properties of data (chapter two). Also, as data may carry personal identifiable information, related to an individual's attitudes, behaviours, actions, characteristics, among other sensitive variables unique to that individual, it is important to consider the privacy implications of data donation, and how individuals may consider them. Also, the considerations of privacy as they were previously discussed, especially privacy as a social value and as contextual integrity inform the how the risks can be constructed by the participants.

This section introduces privacy-specific risks that may be experienced by individuals while deciding whether to donate their personal data by discussing Solove's Privacy Harms Framework (Solove, 2006, 2008). This way, it is possible to explore privacy as an additional dimension, hinted but not explored by Barkworth and colleagues, that may be influence an individual's decision when considering whether to donate their personal data. Therefore, and before discussing the privacy harm taxonomy, it is important to address how Solove dismisses previous privacy theories, and, instead, focuses on developing a taxonomy that encompasses all the possible risks to people's privacy.

3.5.1 A TAXONOMY OF PRIVACY HARMS

Solove argues that privacy is "too complicated a concept to be boiled down to a single essence" (Solove, 2006, pp. 485). He claims that the attempt to conceptualise privacy by finding a common denominator, is comparable to the "search for the holy grail" (Solove, 2008, 39). In fact, this position, that shies away from other scholars attempting to define privacy, derives from Solove's critiques to pre-internet theories, such as privacy referring to the "right to be let alone" (Warren and Brandeis, 1890), or "the right to limit access to the self" (Westin, 1967). Solove argues that these theories, aiming to find a common denominator of privacy, fail by not identifying the premise upon which their theory is built. He suggests that these theories follow the traditional method of formulating a conceptualisation: trying to identify what separates one concept (i.e., privacy) from any other concept (i.e., secrecy).

Even though many authors claim they have identified that common element that, they argue, may be applied to all privacy related situations, there is often a scenario where the definition given is not suitable. For example, the very first definition of privacy as the “right to be let alone” is simply too broad. As Allen (1988, pp. 7) denotes, under this definition, “a punch in the nose would be a privacy invasion as much as a peep in the bedroom” simply because in both scenarios people’s right to be let alone is violated.

Additionally, for Solove (2008), conceptualising privacy as the control over information, as Westin’s theory does, fails by not defining what “control” encompasses. Especially because many theorists view control over personal information as a form of ownership, or an individual’s property (Solove, 2008). If that is the case, then whether it is the individual or the platform who owns one’s data is still being disputed. On the contrary, privacy conceptualised as control over information, can be deemed as too narrow: privacy can be equally breached by any nuisance that disturbs an individual’s serenity, without the need for any personal information about an individual being disclosed (e.g., a man briefly exposing his, or part of his bare body to strangers in a public venue) (O’Brian, 1979). However, even though Solove dismisses most of the previous theories of privacy, his taxonomy is rich in sociality. In fact, Solove (2008, pp. 98, 71) argues that “by understanding privacy as shaped by the norms of society, we can better see why privacy should not be understood solely as an individual right [...] the value of privacy should be understood in terms of its contribution to society”. Accordingly, “privacy is not an external

restraint on society but is in fact an internal dimension of society” (Solove, 2015, pp.80). Thus, the social value of privacy – even when privacy protects an individual, this protection is beneficial to the society as a whole.

Solove looks at privacy as an array of affinities: “privacy is not reduced to a single essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance with each other” (Solove, 2008, pp. 756). Solove following a ‘top-down’ approach attempted to solve this privacy conundrum by drawing general concepts from specific privacy-related situations. This approach led to Solove’s taxonomy of privacy harms. This taxonomy moves past any vague conceptualisations of privacy and focuses on what Solove argues is the most pressing issue privacy scholarship should be focusing on: the potential risks to people’s privacy.

These categories present the five stages of the data processing that may endanger an individual’s privacy: information collection, processing, dissemination and invasion. The data collection stage concerns the way institutions collect personal information (i.e., how is it collected). Information processing refers to how the data is being used by the institution collecting it. Issues, such as identification, insecurity, and secondary use may occur. Identification represents the use of information to identify someone. Insecurity is related with the risk of the data not being secure against improper access. Furthermore, secondary use happens when an agent uses the data for a different purpose from which it was gathered, without the donor’s consent.

In relation to the information dissemination stage, Solove (2008) distinguishes between several potential issues: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion. Breach of confidentiality happens when an organisation cannot keep one's information confidential. Disclosure happens when the information about a person is revealed, affecting their reputation. Exposure refers to when one's personal data reveal something potentially damaging (e.g., an individual's HIV condition). Increasing accessibility may result in sensitive information, beyond what the donor initially agreed upon, being exposed. Blackmail is the threat to reveal private information. Appropriation happens when one's data is used to serve other goals. Distortion involves the propagation of false information about the donor.

Lastly, in relation to the Invasion stage, (Solove, 2008) argues that individuals may be subject to intrusion and decisional interference. While intrusion involves actions that disturb one's peacefulness (e.g., receiving unwanted mail), decisional interferences relate to the meddling into an individual's personal decisions (i.e. trying to condition one's behaviour and actions).

In despite of its comprehensive categorical structure, Solove's taxonomy lacks boundaries. As discussed before, privacy is a highly contextual concept, regulated by different norms of information flow. These may be dependent on many variables, such as, for example, an individual's culture. In 2017, Shivam Bij from the Huffington

Post²⁹ wrote in relation to privacy in India: “What is the meaning of privacy in a country where men don’t mind urinating on the pavements? What is the meaning of privacy in a country where entire joint families live together in small homes?”. What could be perceived in a certain context, under Solove’s framework, as a given privacy harm, in a different context may have a different interpretation.

Solove dismisses this critique by arguing that the definition of boundaries and recognition of nuances is not as important as objectively addressing the spectrum of possible risks to an individual’s privacy. What is at stake, for Solove, is providing a comprehensive framework that can be legally used to help identify privacy harms. Arguably, this taxonomy is key for the study of privacy because it aims to explore each problem and comprehend them clearly, in order to protect individuals facing privacy challenges (Solove, 2008, pp. 759).

Solove’s framework adds an important dimension to the study of data donation. More than discussing the specific categories of harms, it recognises privacy’s role on an individual’s decision to donate personal data. Even though it was conceived as a legal framework, it is now adopted for this study as a key dimension to be explored in understanding how individuals construct the risks of donating their personal data. Specifically, how individuals express, feel, and experience the risks of donating their personal data.

²⁹ https://www.huffingtonpost.in/2017/08/24/indians-don-t-care-about-privacy-but-thankfully-the-law-will-teach-them-what-it-means_a_23179031

3.6 CONCLUSION

This chapter used theory and research about privacy to set out the kind of data that can be donated, and the likely risks and harms individuals are likely to feel as a result of their donation. The insights from this chapter combined with those from chapter two will now be used to set out a study which will investigate the likely risks discussed by individuals when they evaluated whether to donate their personal data. This thesis proceeds to investigate the question: *In the context of a smart city, to what extent are individuals' constructions of the privacy risks associated with mobility data donation³⁰ based on the general risks associated with donation or risks specific to the donation of data itself?*

In the context of data donation, trying to define privacy may not appear as important as understanding the risks that people may construct when donating their personal information. Especially how these risks interplay with the donation-specific risks as discussing in the last chapter. However, discussing different conceptualisations of privacy is key to understand what categories of data can be donated, different attitudes towards data donation, how individuals understand privacy, how is privacy present in everyday life, and its importance for society, relationships, and individuation.

This chapter concludes by discussing Solove's Privacy Harms Framework. His framework provides a comprehensive approach to categorise risks at the different

³⁰ Mobility data as a type of everyday data was chosen to narrow the scope of data investigated. Especially as everyday data encompasses all data that is created during an individual's daily life.

stages of data processing (i.e., collection, processing, dissemination, and invasion), however, it does not address the contextual nature of privacy. In different contexts, to what Solove may classify as, for example, a data dissemination harm, it may not be perceived as such to the individual or social group. Therefore, it is argued that, in pursuance of a more adequate solution to protect individuals' privacy, the focus has to be on the individuals, the ones at the very centre of what we, scholars, privacy advocates, NGOs, activists, legislators, aim to understand and protect. Accordingly, if, in researching privacy, and related topics, people's behaviour keeps being generalised and assumed as predictable, the underlying motivations and nuanced risk perceptions inherent to the individuality of a person, go amiss. This research proposes to look at exactly that. **It aims to understand how individuals understand and argue the risks involved in donating their everyday personal data. In specific, it explores the interplay, if any, between Solove's Privacy Harms framework and the risks associated with the traditional types of donation, as discussed in the previous chapter.**

Chapter 4: RESEARCH METHODS AND DESIGN

4.1 INTRODUCTION

This study focuses on the individuals' construction of risk when considering whether to donate their everyday mobility data to a smart city project. Specifically, it explores how the risks associated with different traditional donations (as per Barkworth et al.'s, 2002 framework) interplay with privacy-specific risks (as per Solove's, 2006 framework) an added dimension of data donation. Studies of data donation have previously focused on discontinuous and unusual life events (e.g., personal data to study suicidal behaviour). There is a research gap concerning the donation of everyday data. Data pertaining to a person's social media interactions, location history, transport used to move within a city can be donated to, for example, smart cities in order to help them improve the public road network, public transportation routes, manage traffic amongst other things. This form of data donation is already practiced in many different smart city projects, such as Glasgow and Milton Keynes. There is not, however, research addressing this particular phenomenon. There is literature addressing similar smart city practices, but they are conceptualised as data sharing or surveillance.

I have decided to focus the investigation of data donation to the context of a smart city, and, in specific to the donation of mobility data. The decision to focus on the donation of mobility data was not only pragmatic in that it restricts this research to a specific scenario but also maps on to one of the categories of data attracting privacy concerns by Finn and colleagues (2013). Furthermore, the phenomenon of data donation, in

particular the donation of mobility data, as a form of citizen participation is becoming increasingly predominant in smart cities (see section 4.3.1). Therefore, it is likely that individuals are able to relate to this scenario. Lastly, as donating data to a local council may have a considerable positive impact in how cities address the issues important to their citizens, data donation is of particular importance to society. Contextualising this study on smart cities, also aids in narrowing the recruitment of participants to a sample of people who commute or move within a city by, for instance, cycling – and may be already used to tracking their routes, amongst other data in applications such as Strava³¹.

Accordingly, this chapter introduces and discusses the philosophy of knowledge adopted by this research and explores the design employed to empirically examine people's construction of risk when considering whether to donate their personal data to a smart city project. It details how the data collection is informed and processed, and justifies the methodology employed in its collection. The chapter starts by considering different ontological and epistemological philosophies and argues for the researcher's stance as a social constructionist. This is followed by the discussion of the methodology employed in the study and its design. Lastly, how the data was analysed, namely the use of thematic analysis is justified as the most adequate to address the research question:

³¹ <https://www.strava.com>

In the context of a smart city, to what extent are individuals' constructions of the privacy risks associated with mobility data donation based on the general risks associated with donation or risks specific to the donation of data itself?

4.2 PHILOSOPHICAL CONSIDERATIONS

Before exploring how this research investigates the research question, it is first necessary to discuss how the researcher's philosophical approach informs the way the research is conducted. This philosophical approach concerns the researcher's belief regarding 'what is reality' (ontological perspective), and 'what we know and how we know it' (epistemological perspective) First, the ontological approach of the researcher is discussed followed by the epistemological perspective. To have a clear epistemological position is essential to a researcher as this will inform the way the data is collected, analysed, and, ultimately, the conclusions reached (della Porta and Keating, 2008). Accordingly, this section serves to instruct the reader of how this research is informed and, serves to contextualise the way the empirical results are going to be analysed.

4.2.1 ONTOLOGICAL CONSIDERATIONS

Ontological perspectives in the social sciences can be understood in terms of a spectrum. Broadly one can distinguish between objectivism, also referred to as realism, in one side of the spectrum and relativism, also referred to as constructionism,

on the opposite side (Bryman and Bell, 2003; Benton and Craib, 2010). Realism “asserts that social phenomena and their meanings have an existence that is independent of social actors” (Bryman and Bell, 2003, pp. 22). This ontological position argues for a reality independent of an individual’s own perceptions and beliefs. It also suggests that an individual’s perceptions and beliefs relate to phenomena external to the individual. For example, gravity exists independently of one’s, or the society’s belief. Relativism, on the other hand, “asserts that social phenomena and their meanings are continually being accomplished by social actors” (Bryman and Bell, 2003, pp. 23). In other words, reality is not independent from the social actors as realists posit, it is being continuously created and revised by individuals through social interactions. Under a relativist ontology, gravity is subjective. It is subjective because it derives from scientific and social conventions agreeing on the concept of gravity. However, Sokal (1996)³² famously argued: “anyone who believes that the laws of physics are mere social conventions is invited to try transgressing those conventions from the windows of my [twenty-first floor] apartment”.

In this thesis, constructions of risk are investigated. Therefore, before moving on to discuss the philosophy of how we come to know what we know (i.e., epistemology), it is first necessary to discuss the ontological status of risk. Namely, is risk a reality independent from the individual or is the individual that constructs that reality? This is a highly debated topic, subject to a widespread disagreement. Mitchell (1999, pp.

³² https://physics.nyu.edu/faculty/sokal/lingua_franca_v4/lingua_franca_v4.html

165), whose risk framework is adopted by Barkworth and colleagues to the study of donation risks, decides to bridge both ontologies arguing that “unlike many subjects which divide researchers along the lines of how they view the world, perceived risk encourages a convergence of these divergent views”. He believes that objective risk must exist - physical, time, financial risks can be measured. Conversely psychological risk, for example, seems to be an exception, on the lines of a more subjective risk. To Mitchel it is important to be able to measure subjective risk, as is the case of the psychological risk. Mitchel (1999, pp. 165) continues by arguing that “for realists to concede that the subjective impressions of an observable phenomenon are worth conceptualising and measuring is a major bridge of the philosophical divide. Equally relativists seem happy to concede to the use of the scientific tools of the realist to analyse risk, philosophically secure in the knowledge that it is an individual and relativist perspective which is attempted to be measured”. For example, in the specific case of psychological risk, psychometric scales can be used to measure this factor. For Solove (2002, 2006) the privacy harms are also objective reality. In other words, one’s privacy may be invaded whether an individual understands it as such or not – providing an interesting argument when comparing to the concept of felt risk or vulnerability discussed in section 3.4.

This thesis, however, does not agree with Mitchell on his argument about the ontological status of risk. Notwithstanding the fact that risk may be accepted as an objective reality, risk perception and construction ought to be studied as a relative construct. For example, if an individual commutes every day by car there may be a quantifiable risk of having an accident. However, that has nothing to do with the

driver's perception of that risk, and how they may describe that risk to others during the course of social interaction - which Mitchel himself recognises (pp. 165). The individual's perception is relative to their construction of the risk. For instance, someone who experienced a car accident may construct different risks of driving than someone who never experienced an accident. The life experience is a subjective element playing into the individual's construction of that risk. The same example can be given when discussing data donation. If an individual expresses, for example, a risk related to the dissemination of their data is because they constructed it through social interactions or life experience.

Delving into a philosophical debate on the existence of risk is not what is intended. Instead, the way the researcher understands the concept of risk perception is explored as it is vital for the interpretation of the methodology, empirical examination of the phenomenon, and subsequent discussion. Accordingly, this thesis concurs with Dietz, Frey and Rosa's (2002) argument that "people do not see the world through 'virgin' eyes but filtered through social and cultural meanings, which are conveyed by primary sources such as family, friends, superiors and colleagues". Furthermore, it agrees with Douglas and Wildavsky's (1982) thesis that risks are defined and perceived differently by people in different social contexts. After justifying the ontological status of risk and risk perception in the literature, adopted frameworks, and the position of the researcher, the section below introduces and discusses different theories of knowledge and argues for the adopted epistemology of this thesis.

4.2.2 EPISTEMOLOGICAL CONSIDERATIONS

Epistemology is the theory of knowledge. It discusses how we know what we know. Positivism, for example, is an epistemological approach based on a realist ontology. It postulates that “knowledge is arrived at through the gathering of facts that provide the basis for laws” and that “science must (and presumably can) be conducted in a way that is value free (that is, objective)” (Bryman and Bell, 2003, pp. 16). Therefore, to gather facts, be value free and objective it is necessary to disregard the individuals’ beliefs, cultures, opinions, among other variables that makes them, inherently, subjective.

Social constructionism, an epistemological approach based on a relativist ontology, postulates that, in order to investigate a phenomenon, it is necessary to investigate the actors that are involved in the creation of such phenomenon. Social constructionism argues that “understanding, significance, and meaning are developed in coordination with other human beings” (Amineh and Asl, 2015, pp. 13). This assumes that human beings rationalise their experiences by creating a concept of how the social world works, and that language is the fundamental form in which individuals construct reality (Leeds-Hurwitz, 2009; Spector and Kitsuse, 2001). This research adopts a social constructionist approach as it looks to understand the ways individuals construct the risks of donating personal data. In other words, this study aims to uncover the social phenomenon of risk perception as constructed by individuals through interaction with others, and their own personal experience when considering data donation.

There are two main divisions of constructivist theory that are often misunderstood and wrongly used interchangeably that ought to be considered. Social constructivism and social constructionism. Guterman (2014, pp. 13) explains the difference by claiming that: “although both constructivism and social constructionism endorse a subjectivist view of knowledge, the former emphasizes individuals’ biological and cognitive processes, whereas the latter places knowledge in the domain of social interchange”. In other words, both maintain that knowledge and reality are subjective. However, whereas constructivists believe that knowledge and reality are created within individuals (i.e. brain’s physiology), social constructionists contend that knowledge and reality are constructed through discourses and social interactions.

As argued in the previous section, it is still highly debated whether risks ought to be studied either as if they were a material reality or socially constructed. This thesis concurs with Douglas and Wildavsky’s (1982) and Davis (2008), in that the perception of risk is a complex construct embodied in social discourse. Individuals use language to produce a risk analysis, which will lead to certain actions, or decisions, that form a risk (Giddens, 1990; Russell and Babrow, 2011). Therefore, investigating and conceptualising risk as if it is a material reality (e.g. Beck, 1992), leads to a scientisation of occurring social phenomena (Luhman, 2002). Luhman critiques those who employ quantitative methods to explore risk and risk perceptions, claiming that “the more we conceptualise and quantify the constructs we posit as risk, the further we move from uncovering the essence of human experience” (Russel and Brabow, 2011, pp. 244).

The approaches taken by the studies and frameworks underpinning the donation risks adopted by this thesis are positivist – Barkworth et al. (2002) adopted Mitchell's (1999) risk perception framework to donation studies. Barkworth and colleague's (ibid) framework attempts to categorise how people are likely to perceive donation risks a priori. It classifies these perceived risks by dividing them in different categories: physical, psychological, social, time, performance, and financial. This study strips the objective essence of Mitchell's (ibid), and to the same extent Barkworth and colleague's, framework and applies the proposed categories in understanding how these interplay with the privacy-specific risks by focusing on the discussion and interplay of arguments by the participants.

After critiquing approaches to risk research, and examining the reasoning of this thesis, it is now important to focus on privacy research, another key element of this thesis. Studies of privacy and privacy risks do not tend to adopt a constructionist approach (e.g., Acquisti and Grossklags, 2005; Jensen et al., 2005; Baek et al., 2014; Blank et al., 2014). Methods such as large-scale surveys (e.g., Acquisti and Grossklags, 2005; Baek et al., 2014; Blank et al., 2014; Krasnova et al., 2009), and experiments (e.g., Hann et al., 2007; Jensen et al., 2005; Sundar et al., 2013) are amongst the most used when investigating privacy related phenomena, which represents a positivist, hypothetic-deductive approach. However, the problem with these approaches in privacy scholarship is that large scale surveys and experiments do not explore the world as seen through the eyes of those who experience privacy and its violation – it simply does not address the subjectivity of human experience. Accordingly, positivist studies into risk and privacy phenomena provide a broader template against which one

can understand how people make sense of risks whilst this study provides latitude for sensemaking.

Notwithstanding the potential benefits a positivist approach might have for privacy and risk research, the interest and focus of the researcher is in analysing the claims made about the risks of data donation. The researcher aims to analyse the intensification and mitigatory arguments through social interaction in search for patterns in the perception of risk. The aim of this research is not to address the validity of those patterns. In fact, focusing on the argumentation of the participants directs the analysis towards the employment of language and communication patterns. This is particularly important in a social constructionist approach as language is key to access the reality constructed. Accordingly, to address this inherent subjectivity of the construction of risks of donating personal data, and in order to draw on the richness of personal experience, the researcher looks to uncover and understand the risk perception patterns through the analysis of verbal communication. The section below explores the research design of this study.

4.3 DATA COLLECTION METHODOLOGY

The present study takes a qualitative approach as it focuses on the subjectivity of privacy and risk constructions, by pursuing an in-depth knowledge of the phenomenon studied within the context of individuals' experiences, attitudes, and interactions. This section presents and discusses the methodology used to collect the data that enables

the identification of the argumentative patterns surrounding the construction of risk related to the donation of data.

This study investigates how individuals construct the risk of donating their personal data to a smart city. The use of social constructionism provides an appropriate approach in understanding how individuals construct the risks involved in donating their personal data based on their experiences, attitudes, and beliefs. Nonetheless, the use of social constructionism is usually associated with an inductive reasoning approach where the researcher aims to make broad generalisations from data observed and other specific premises. For instance, if an individual takes several consecutive pennies from a wallet, one can induce that in the bag there are only pennies. In other words, it observes a specific pattern and draws a generalisation based on that specific pattern. This research, however, observes an abductive reasoning. It looks at a priori categories and bases the empirical test and analysis in relation to these categories, notwithstanding the possibility of new categories appearing in the data. It has deductive and inductive elements, while exploring risk through a constructionist lens. Through an examination of the literature, a theoretical framework was deduced.

In other words, this study explores the subjective essence of risk perception with an established frame of reference (i.e., the traditional donation risk categories). From here, an exploratory (inductive) qualitative empirical study was conducted, and the best possible reasoning derived (deductive). Accordingly, this study can be considered as following an abductive reasoning as it starts from incomplete observations of the phenomenon (through the empirical study), then moving through an inductive

reasoning (through an exploratory study), and from here derives the conclusion, based on the observed patterns, which were analysed through a previously clearly defined framework. As such, the unit of analysis (i.e., the ‘what’ is being analysed) are the participants’ argumentative patterns that relate to risk. In specific, how individuals identify, intensify and mitigate different risks of data donation, as well as the basis for those justifications.

Data donation is a wide subject encompassing many types of data, and many types of donation contexts and scenarios. Therefore, to better explore the phenomenon of data donation, it is necessary to narrow the scope of this research in order to focus on one specific context. This will not only allow the researcher to account and control for arguments akin to more extreme scenarios, as, for example, medical data donation in which the communication for its need is rooted on the premise of advancing science and saving lives but will also allow the participants to engage in a discussion that they may be familiar with. For example, donating personal data from someone who is clinically depressed or attempted suicide to an organisation such as OurDataHelps.org³³ may be a one-time only, sensitive³⁴, example of data donation. This example represents the donation of data under exceptional circumstances. Conversely, donating mobility data to a smart city project may represent a more mundane, everyday activity rather than representing exceptional circumstances as argued in the last example.

³³ OurDataHelps.org is an organisation to which people can donate their personal data or of those who experience depression or committed suicide. Their goal is to research online behaviours and attitudes that may predict suicidal tendencies.

³⁴ This sensitivity in data donation arises from the activity that the data represents

The research began by conducting key informant interviews with experts working in the smart city context. The purpose of the key informant interviews was to understand the role of data donation in smart cities. The main body of the research drew on data collected in focus groups with vignettes used as stimulus material. Focus groups were considered appropriate for eliciting discursive data because it allows for the participants to exchange arguments based on experiences, attitudes, and beliefs. Accordingly, there is place to a rich interplay of arguments relating to the social construction of data donation risks, that one would otherwise miss with, for example, interviews.

4.3.1 KEY INFORMANT INTERVIEWS

In order to better understand the issues that might shape data donation in the smart city context, it is necessary to explore how smart city projects work - how they operate, how they gather data, how do the citizens participate, amongst other things. Accordingly, key informant interviews are the ideal method to understand how data donation works in a smart city. Key informant interviews are qualitative in-depth interviews with people who have expertise in a particular area, subject or phenomenon. The purpose of these interviews is to collect information and advice regarding the issue being studied (Carter and Beaulieu, 1992). Key informant interviews were conducted in order to understand the smart city ecosystem and the role data plays in that ecosystem. Also, these interviews were conducted in order to understand how data was being collected and how donation functions in the smart city context.

As this research decided to focus on Milton Keynes Smart City Project (MK: Smart), two researchers from the Open University (OU, located in Milton Keynes) actively involved in the project were contacted in order to understand their availability and willingness to discuss in more detail the MK: Smart project. The introduction to these researchers was facilitated by my supervisor who has previously worked at the OU. The interviews were semi-structured. However, there were a set of guiding open-ended questions, which can be examined on annex 1, with the objective of understanding how the MK: Smart project works, how is data collected, how is data being donated, in what contexts, and how are the data donors being recruited to participate in the project.

A wealth of different smart city features, technologies, and criticisms were explored during these interviews. For example, how sensors are used in buses to advise people waiting of the capacity of the bus, where it is or how late is it and how full they are. This may help individuals plan alternative forms of transportation, or even when to get out of home so they do not have to wait for a long period of time. Similarly, sensors were implemented in shopping centres to inform citizens of how busy certain stores are at any given moment. Technology was deployed in people's homes to inform them of their energy, and water consumption. This program would, for instance, be able to advise citizens about when to water, or not, their gardens.

MK: Smart partnered with a local organisation – Community Action: MK – to help spread the word about these initiatives while making it easier to recruit individuals willing to participate. Through Community Action: MK, the MK smart city project

recruited citizens to their data donation initiative: Redways Reporting App. ‘Redways’ are the cycling paths connecting most of the city. This app allows users to report problems with the road conditions based on their location and photographic evidence. This initiative was integrated within a much larger data donation project, as explored in the introductory chapter of this thesis, entitled “MotionMap”, where individuals could give their location data, speed, amongst other types of data. This would then help the city council plan the road networks, and feed information back to users regarding the best routes to take, for example.

These interviews helped understand how smart cities work, and, in specific, how data donation happens in a smart city. In this context, and aligned with the research question, what demanded investigation was how citizens construct the risk of giving their personal data to their smart city. Therefore, capitalising on the extensive experience of Milton Keynes as a smart city, focus groups were conducted with their citizens, or individuals who frequently commute to Milton Keynes as to capitalise on their experiences of living in a smart city. Nonetheless, before discussing focus groups as the chosen method for data collection, further information regarding Milton Keynes, including the relationship its citizens have with the local government, will be provided.

4.3.2 MILTON KEYNES

Milton Keynes, situated in Buckinghamshire, roughly 80km to the north-west of London, was created in the 1960s with the purpose of alleviating the housing pressure

in London. According to the Office for National Statistics³⁵, in mid-2019, Milton Keynes had a population of roughly 269 500 people, from which 26% is classified as ethnic minority. Milton Keynes has an area of 30 862 hectares, comprising of 48 parishes, making it the largest town in Buckinghamshire. Furthermore, whereas the majority of older cities in the United Kingdom were planned according to a radial pattern, Milton Keynes was planned according to a grid pattern layout. This one-of-a-kind layout in the country with its proponents arguing that it facilitates the flow of traffic and frees the residential areas from noisy congestions.

Alongside the well-defined road network, a dedicated network of cycling and walking paths was planned and built throughout Milton Keynes, as previously mentioned, called 'The Redways'. Currently, there are over 200 miles of these paths. According to MK: Council, cycling has doubled since 2010 with The Redways being a key factor in the uptake of cycling in the city. In figure 7 below, The Redways network is pictured.

35

<https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland>



FIGURE 7 - THE REDWAYS NETWORK

Source: Get Smarter Travel MK

Milton Keynes has a close relationship with its citizens. In partnership with Community Action: MK³⁶, as discussed in the above section, the city council has maintained close ties with the community. According to Community Action: MK's website, they act in three spheres. First of them being 'mobilising communities' as they work toward bringing people together in their communities while offering support in any collective action they might need. Second of their core spheres is 'strengthening groups' as they provide advice with governance, funding and development. Lastly,

³⁶ <https://communityactionmk.org>

with ‘shaping decision making and policy’, the volunteer group works with communities to ensure their opinions and experiences is taken into account at a local and national government level. They state that “all of their work is focused on the elements of strong, resilient, sustainable communities” (communityactionmk.org).

However, despite the close ties with the community, in 2011, Milton Keynes Council found itself in the middle of a scandal after leaking the personal data (addresses and phone numbers) of 50 residents³⁷. This event may have an impact in the results of this study as it can influence participants’ perceptions of how the smart city project will handle their personal data. Although the issue of institutional trust is one that warrants further research, it is not the focus of this research.

4.3.3 FOCUS GROUPS

Once the key informant interviews were complete, a focus group design was chosen for the main body of data collection. Focus groups are also often referred to as group interviews (Morgan, 1997). Despite being referred to in this way, an important distinction remains between focus groups and group interviews: while all focus groups are group interviews, not all group interviews are focus groups (Frey and Fontana, 1991). Morgan (1996, pp. 130) defines focus groups as a: “research technique that collects data through group interaction on a topic determined by the researcher”. This definition provides the three main characteristics of focus groups. First, focus groups

³⁷ <https://www.itpro.co.uk/633649/ico-called-on-to-punish-milton-keynes-council>

intend to generate and collect data. Second, the means by which the data is sourced is through interaction in a group discussion. And, lastly, it recognises the researcher's active participation in starting and placing the discussion by setting a theme (Morgan, 1996). Focus groups and group interviews differ in the way they are conducted, and their purpose. Gibbs (2012, pp. 186) makes the distinction by claiming that "group interviews are a way to gather many opinions from individuals within a group setting but are largely didactic between interviewer and each individual in the group. The distinguisher of focus groups is that they are interactive [...]". In a focus group, the researcher's role is to moderate the discussion ensuring that the discussion remains within topic. In the case of group interviews, the interviewer plays a more central role in the way the interview is conducted by asking specific questions directly to the participants. Furthermore, Morgan (1996) claims that the purpose of focus groups is research. The purpose of, for example, group therapy, brainstorming sessions, recruitment interviews in groups is something other than research. Therefore, according to Morgan's argument, they cannot be considered focus groups, but group interviews.

Unlike some positivist approaches, such as surveys, where the size of the sample needs to be large enough to offer a stronger statistical significance, focus groups and other qualitative methods are not bound by the same requirement. The interaction between the participants is what will generate the dataset. Therefore, the number of participants is limited by the method itself. A higher number of participants in a focus group would limit the active participation of some individuals. For example, if a focus groups is too large, the participants might not feel at ease to talk and discuss certain topics that may

be more sensitive. In order to create an optimum level of interaction between individuals, Morgan (1996) suggests that focus groups should range from four to twelve participants. Although, according to Morgan (ibid), the total number of focus groups in the majority of studies should range between four and six, as, usually, by then saturation is reached. However, if the study is segmented, for example, by gender, the number of focus groups conducted may increase according to the number of segments explored, and the geographic area covered.

Focus groups are an appropriate data collection method for this study because individuals construct notions of risk by, not only relying on their own experiences, but also by being influenced by other's discourses, including people with which they come into contact as well as those which feature in the news and other media. Focus groups enable the researcher to observe how, through interaction, the participants' views are established, stabilised, debated and challenged. Lastly when appropriate stimulus materials are used in a focus group setting, participants experience a genuine conversation with their peers. The researcher is present to facilitate discussion in a way which encourages participants to share their views and hear the views of others in relation to the matters at hand (Greene and Hogan, 2005).

Focus groups were chosen over in-depth interviews for a number of important reasons connected with the research question. The research aims to understand how the risks associated with data donation are constructed. Although in-depth interviews allow for a deeper understanding of the individual, they are less effective at capturing the social construction of data donation risks that are constructed as part of a conversation

process. The reason for this is that on an in-depth interview, the researcher is only generating data from the experiences and attitudes of that one individual, without being subject to the rich social interaction that one can experience in a focus group setting. As Hennink (2014, pp. 2-3), puts it: “perhaps the most unique characteristic of focus group research is the interactive discussion through which data are generated, which leads to a different type of data not accessible through individual interviews. During the group discussion participants share their views, hear the views of others, and perhaps refine their own views in light of what they have heard”. Observing a focus group discussion means that the researcher is overseeing how risks are socially constructed in conversation and will depict the interplay between the types of risk with which the participants are concerned. The focus group discussion enables the generation of data about this research’s unit of analysis – the social construction of data donation risks – so that I can then understand the factors which influence the individuals’ conceptions of these risks and then analyse the data. I do this by introducing stimulus material appropriate to the phenomenon under study.

Stimuli supports the focus groups discussions by directing the discussion taking place. Several types of stimuli may be used to elicit discussion in a focus group setting: videos, simulated environments, theatrical pieces, tasks, audio clips, vignettes, and many others. However, for the particular issue being addressed, the use of a written vignette is appropriate because it illustrates how data donation would fit into everyday life. Below, the use of vignettes as stimulus material to elicit discussion pertaining to the risks of donating data to a smart city is explored and justified.

4.3.4 VIGNETTES

The focus group methods used in this study featured a series of vignettes about data donation in everyday life. Vignettes are “short scenarios in written or pictorial form, intended to elicit responses to typical scenarios” (Hill, 1997, pp. 177). A rich discussion is crucial in yielding language patterns. In this research, the patterns that refer to individuals socially construct the different risks of donating personal data – this thesis’ unit of analysis. Vignettes work to focus the discussion on the phenomena under investigation. Vignettes help foment and uncover the way participants socially construct risks and how the interplay of arguments unfolds (Hughes, 1998). It is due to this particular characteristic that vignettes have been widely used by researchers aiming to examine the complexity of social aspects (Barter and Renold, 2000).

As data donation outside the medical context is a novel concept, it is important to acknowledge that the participants may not be sufficiently informed about the particular issue being discussed. They may even confuse data donation from data sharing and base the majority of their arguments on news (e.g., Facebook Scandal), and their experiences of using social media platforms. It is vital that the vignettes presented are consistent and can be easily followed and understood by the participants (Barter and Renold, 2000). Furthermore, it is equally important that the vignettes presented are authentic and illustrate reasonable scenarios to the participants (Neff, 1979).

The decision to use vignettes, instead of directly asking questions to the participants, is due to how sensitive privacy and its surrounding issues may be to some. Vignettes are often used in sensitive settings to mitigate potential psychological harms of asking

the questions directly to the participant (Neale, 1999). Therefore, instead of feeling obliged to discuss their personal experiences, the participants can comment on the story and thus feel more at ease. It also allows the participants to have a greater control over their participation as they may choose whether they would like to discuss their own experience to illustrate and reinforce their responses (Barter and Renold, 1999, 2000). Accordingly, vignettes are employed in this research as it protects participants by “placing distance between their experience and that of the vignette character” (Cradbury-Jones, Taylor and Herber, 2012, pp. 427).

Due to the novelty of data donation, devising accurate scenarios, which individuals can easily picture, proves to be a major challenge. The vignettes ought not to illustrate a conceptualisation of data donation as a future dystopian practice, nor as necessary to a well-run, efficient local government. Instead, they must provide a neutral conceptualisation of what data donation on a smart city context encompasses and how it can be used – both touching positive and negative spheres – by the local authorities.

Despite the clear advantages of applying vignettes to this study, there are some theoretical and methodological limitations. First, the issue with the ‘distance’ between the scenario and ‘reality’ may limit the discussion. As Barter and Renold (2000, pp. 311) put it: “what people believe they would do in a given situation it is not necessarily how they would behave in actuality”. However, the discrepancy between beliefs and practices should not be cause for concern since outcomes will always be context dependent. Given that this thesis adopts a social constructionist approach, what really is important is the process of meanings and interpretations used by the participants to

arrive at a given outcome (Finch, 1987). Second, it may be argued that vignettes are not able to duplicate the complexity of social reality. Therefore, meanings and interpretations might be attached to something that does not feel real to the participant, thus the appropriateness of the use of vignettes for this research. Moreover, none of the findings can be generalised (Barter and Renold, 2000). Nonetheless, this research does not attempt to provide the scholarly community with a generalised contribution. That would be a deductive reasoning approach, where one goes from a broader premise to a specific conclusion.

Instead, this research accepts the limitations that the conclusions can be generalised only to a certain extent. Accordingly, Corkery (1992) suggests the use of vignettes in focus groups since it provides a flexible approach that allows for an isolation of specific phenomena, such as the social construction of data donation risk. In making this statement it is acknowledged that no research methods can completely capture the complex nature of social systems (Barter and Renold, 2000).

Studies into the social construction of risk have often adopted the use of vignettes (see Austen, 2009; Pilkington, 2007) as it helps enrich the discussion around particular risks in specific contexts that the researcher aims to explore. For example, Austen (2009) used vignettes in order to investigate how young people construct risk, especially risk surrounding the consumption of drugs and alcohol. For this, Austen employed a set of five written vignettes, within each of the five vignettes there were three scenarios that were based on features of risky decision making relating to the use of cannabis. These vignettes were all pertaining to the different constructs that the

researcher was investigating. For example, was risk perceived as a negative concept? Did students take teacher's information regarding drugs as a fact? Amongst others. One of the vignettes portrayed a young individual facing a decision surrounding 'risk information': Would the young individual believe the teacher's information about the risk of using drugs, or their peers who claim that they have tried using drugs and suffered no repercussions? Even though the discussion was almost consensual in that "the experiences of peers had a limited effect on the acceptance of knowledge gained from an expert" (Austen, 2009, pp. 18), the vignettes created a rich discussion around the construction of the perception of risk and influential actors in the process (e.g., teachers, media, researchers).

In conclusion, the use of vignettes in a focus group context proves very useful to the study of a wide range of social issues. Specifically, it proves useful in understanding the complexity of the social construction process of data donation risks. It proves especially useful because it assists in unpacking the interplay of different argumentative patterns surrounding risk. Accordingly, in order to clearly address the aim of this research – to understand individuals' construction of potential data donation risks – it is necessary to provide the participants with scenarios where data donation plays a central role. The section below discusses this research's design by exploring the sampling, access strategy, focus groups' structure, amongst other things. In section 4.4.2 the design of the written vignettes is discussed.

4.4 METHODS DESIGN

Following the presentation and discussion of the methodology employed in the study, this section details the design and the different stages of the data collection process. It starts by introducing and discussing the sampling and access strategy.

4.4.1 SAMPLING AND ACCESS STRATEGY

This study focuses on how individuals construct the risk of donating their personal mobility data to a smart city project. However, as previously argued in chapter two, which conceptualises everyday data donation, and chapter three, which sets out the categories of personal data which attract privacy rights, this seemed to be a quite broad subject as there are many types of data that can be donated. For example, health, behaviour, and mobility data are just some of the examples. For this reason, the study was narrowed down to focus on the donation of, primarily³⁸, mobility data, as it is a type of data heavily targeted by smart city projects (as discussed by the key informants – refer to section 4.3.1). Mobility data has been used by smart cities to study, amongst other things, the population's transportation patterns, in order to improve the efficiency of its public transportation. However, in order to narrow even further the population in study, since there are several ways an individual can move within a city (e.g. cars, buses, trams, metro, bicycles, motorcycles, taxis), the researcher decided to focus on

³⁸ Primarily mobility data since collecting only one type of data without collecting other types of data, such as, for example, demographic data, is practically impossible.

the donation of data pertaining to people who cycle, to commute or for pleasure. The decision to focus on this type of data being donated was pragmatic in the sense that it is a type of data already subject to donation initiatives (as discussed by the key informants – refer to section 4.3.1). Also, individuals often engage in tracking their own performance (itinerary, speed, heart rate) by using apps such as Strava, thus, participants would possibly be familiar with some of the technologies involved.

It was necessary to recruit participants who live in, or commute to, a city where there is an active smart-city project. Glasgow and Milton Keynes were both considered as they are both engaged in promoting mobility data donation. However, the decision to discard Glasgow and choose Milton Keynes instead was pragmatic in that the Glaswegian accent could prove challenging when it came to the transcription and analysis of the audio data. Also, due to my supervisor's network in Milton Keynes, it would be easier to access facilities where to conduct the focus groups and to contact key informants from the smart city project. Therefore, the choice of 'smart' city where to focus the recruitment of participants was pragmatic. In its promotion of mobility data donation, the city council is asking individuals who cycle to work to download an app to track their route. In fact, users are not only able to track their route but also can advise where there are issues that they would want fixed (e.g., a pothole, poor street lighting). This particular programme is ideal to provide context for this study as it asks citizens to donate their mobility data as part of their participation in the smart city project.

The focus group sample comprised of adults, aged between 35 and 49, who live in or commute to Milton Keynes and often cycle for commuting or pleasure purposes. The reasoning behind this specific sampling strategy is that, according to a report by the British Department of Transport (2018), cyclists aged 30 to 39 and 40 to 49 were the two age groups who made the most cycling trips in 2017. Overall, cycling enthusiasts made an average of six trips per week. The most commonly reported purpose for the cycling trips was commuting or business (37%). Also, a sample with individuals aged from 35 to 49 offers a broad enough segment without compromising the homogeneity within the group. This homogeneity facilitates a discussion to “flow more smoothly” (Morgan, 1996, pp. 143). Regarding gender, as explained in the next section, there is a balanced number of males and females, in order to guarantee symmetry between groups. In sum, participants were recruited based on their gender, age, geographical location, and their bicycle usage. This segmentation excludes views of other individuals who do not cycle, and, that in consequence, might have completely different views and arguments when discussing the specific scenarios presented. Furthermore, as this research is of qualitative and exploratory nature, the researcher understands that the findings cannot be generalised, therefore, the sample is not argued to be representative.

Participants were selected by an established recruitment company that was previously used by the author’s supervisors – the specific questionnaire used to recruit participants can be found in appendix 2. Due to the fact that Milton Keynes is not easily accessible from the researcher’s location, and, due to the fact that the target sample is somewhat narrow, the employment of a recruitment agency was essential.

Local knowledge, contact databases, and the ability to distribute leaflets advertising the recruitment throughout local venues while respecting people's data, as per the GDPR norms, were some of the parameters taken into account in the selection of the recruitment agency³⁹.

The focus groups took place at the Open University, in Milton Keynes. Colleagues from the Open University agreed in liaising with the administrative staff in preparing the author's status as a visiting researcher, and, henceforth, the room booking process was simple and straightforward. Besides the colleagues facilitating the booking of the venue, the Open University was chosen mainly due to the fact that it is within easy access for the participants, it is accessible for those with mobility difficulties, it has parking facilities for those choosing to drive, and the rooms were equipped with the necessary materials to conduct a focus group (e.g., white board, large table, air conditioning).

Initially, as an incentive to participate and as a mark of gratitude and respect for their time and willingness to participate, £30 'CycleChoice' gift card were offered. This incentive also served to help the participants with any expense they would incur while traveling to the venue. Not offering an incentive would be perceived as exploitative by both the participants and the recruiter. However, with this amount and form of incentive, the agency reported difficulties in recruiting the participants. Adopting the

³⁹ The recruitment agency employed was QRS Market Research, previously vetted by the University of St Andrews as a trusted services supplier.

agency's advice, after seeking the appropriate budgetary and ethical approvals (appendices 5 and 10), the incentives were increased to £40 in cash.

4.4.2 PRODUCING THE VIGNETTES

Barbour (2007) argues that there are no strict rules guiding the design of the vignettes for a focus group. Instead, a reflection on what the study is aiming to achieve is sufficient to the development of the vignettes employed. Nevertheless, although there are no strict rules, a number of guidelines were followed in order to assure that the vignettes were valid and relevant to foment an appropriate discussion around the phenomenon studied. First, the vignettes ought to be representative of circumstances that represent participants' experience and the research question being explored (Flaskerud, 1979). Second, the researcher should consider the characteristics of the participants so that they can match them with the most appropriate type of vignettes (Weisman and Brosigle, 1994). For instance, pictorial vignettes may be more useful for focus groups where the research topic may be difficult to explain to the audience (e.g., children). Furthermore, vignettes that "engage participants' interest, are relevant to people's lives, and appear real" are presumably more effective (Hughes and Huby, 2004, pp. 40). Equally, vignettes followed by open ended questions have considerable value in fomenting the focus group discussion (Sheppard and Ryan, 2003; Hughes, 1998). Vignettes should also be piloted prior to its application in any research, as is the case of most other research methods (Hughes and Huby, 2004). Lastly, in order to establish the internal validity of the vignettes Gould (1996, pp. 211 – 212) proposes,

amongst other things, that these be vetted by an expert that is able to judge their “suitability for the study”.

Considering all the previous elements discussed, the vignettes in this study take form of short prompts depicting an evolving decision-making scenario where an actor decides whether to donate his or her data in different contexts. As Kinicki and colleagues (1995) argue, these short prompts (i.e., paper stories) demand a lower cognitive effort from the subjects when comparing to, for example, a video-vignette, where the participants may derive their own understanding based on other, perhaps ambiguous, cues. In fact, Hughes and Huby (2004, pp. 38) claim that “videotaped or live events require participants to draw their own meaning from observations to a greater extent than written vignettes that are unambiguously processed in the mind”.

When donating data, individuals may construct risks in different ways. For example, individuals may understand that donating data takes a certain amount of time that they are not prepared to spend (i.e., Barkworth’s time risk). They may perceive that their donated data, if in the wrong hands, may bring financial upsets (i.e., Barkworth’s financial risks, and Solove’s disclosure risk – part of data dissemination). Individuals may conceive that, their donated data may lead to a certain exposure (i.e., Solove’s exposure risk) of their physical status (e.g., how fast they cycle, their heart rate, etc.). Nevertheless, there may be arguments to mitigate these risks. For example, individuals may want to help improve the city’s road network, they may want to help develop a cycle route network, amongst other things. The purpose of the vignettes employed in this research is to foment a rich discussion that will elicit these types of arguments.

Accordingly, this debate helps generate meaningful data related to the process through which the risks associated with data donation were socially constructed in the focus groups. To the researcher, this debate allows for an observation of social constructions that, once uncovered and analysed, provide with an understanding of how individuals construct the risks of donating their personal data.

Furthermore, the vignettes were conceived with the type of participants in mind in order to appeal to their interest (i.e., cycling), are relevant to people's lives (i.e. using an app while cycling for commuting or pleasure) and are appropriate to their context (i.e. participating in a smart city programme). The written vignettes were composed with the purpose of eliciting talk about the social construction of risks and the different arguments about the degree of risk that was presented in the vignettes. However, before deciding to use them in the empirical study, vignettes were first piloted within my personal and professional network in order to make sure they were appropriate, consistent and easy to understand. A number of individuals discussed the subject as it was foreseen and understood the concept behind data donation. However, there were few issues raised, especially connected with the way the scenarios were presented and the type of language used. For example, using a fictitious name for a city created some confusion and a suitable explanation had to be given, thus interrupting the flow of the interview. An introduction was added to explain that the name of the city and the name of the character, 'Kris', were purely fictitious and only for the purpose of the focus groups discussion. Furthermore, there were some grammatical errors in the written vignettes that were promptly corrected. Lastly, the vignettes were shown to both my

supervisors that agreed on their suitability for this study, and, later, to the ethics committee that agreed on their ethicality.

In regard to the vignettes, four were conceived with the objective of telling a story. The story was constantly evolving with each vignette, similar to the method used by Austen (2009). The focus of the vignettes is on a central character: Kris. The name Kris was chosen as it is a gender-neutral name, thus allowing the participants to be more comfortable in discussing the scenarios without being confronted with a pre-determined choice of gender for the vignettes. The choice of a gender-neutral name was also made in the interest of adopting a more gender-inclusive research approach. Furthermore, it is one less variation to be accounted for in that all focus groups discuss the same character with no gender determination and possible preconceptions. The particular vignettes used can be found in appendix 3.

The first scenario depicted a situation where an individual named Kris is presented with the opportunity to donate their mobility data. There are no value assessments included in any vignette. This way the participants will not be swayed by these potential value judgements included in the vignette itself. The participants were then asked what they think Kris should do. This allows for an abstraction of looking into possible consequences in relation to their own lives and social roles (e.g. mothers, fathers, teachers, engineers, etc.) and focus on Kris (Bank clerk, cycling enthusiast). Accordingly, asking the participants to take Kris' perspective, is intended to reduce social desirability bias in the participant's discourse in relation to a sensitive topic, as are people's attitudes towards privacy (Hughes and Huby, 2004; Fisher, 1993).

The next vignette is an evolution of the first scenario. This time, the subject is still not sure whether to donate their data. They contemplate some of the possible positives and negatives of participating in the smart city project by donating their data. For example, the app could ensure Kris warns other cyclists of potholes in the cycling lanes, however, should Kris have to stop every time to report that pothole it would prove a time-consuming task. The participants are then asked what they think the subject will do and why.

In the third scenario, the city council provides a fitness tracker to Kris under the pretext that by tracking the heart rate, weight, and itinerary, they are able to understand which parts of the cycling network demand more physical effort from their citizens. This way, they could improve the road network, as well as provide feedback to citizens who have the app about where it might be difficult for them to cycle through. Then, similar to the previous vignettes, participants are asked whether they think Kris will still want to participate in the smart city project by donating their personal data. This vignette intends to exacerbate the conditions under which the data donation occurs. This way, the interplay of arguments may be more intense and patterns pertaining to the construction of risk may come to the fore.

The last scenario illustrates the subject experiencing a consequence of having donated their personal information. For instance, a raise in their insurance premium due to erratic driving behaviour. This consequence is designed according to a risk that could be interpreted through Barkworth's or Solove's framework, or both. The intention

behind these scenarios is to elicit a discussion based on the potential risks of donating data and understand how the participants continue constructing their arguments when the subject of the vignette faces a clear aggravated consequence of engaging with the smart city project.

4.4.3 FOCUS GROUPS DESIGN

4.4.3.1 FOCUS GROUPS COMPOSITION

Powell and Single (1996) argue that the optimum number of focus groups is dependent on how complex is the subject being investigated. In a study by Guest et al. (2017), 80% of literature reviewed reached theoretical saturation with two to three groups. However, the authors argue that it is strongly dependent on many factors, such as, the degree of heterogeneity within groups, the complexity of the theme being explored (also argued by Powell and Single, 1996), the size of the group, and whether or not the conditions vary within or between groups may all impact the number of focus groups necessary to reach theoretical saturation. Due to the fact that the focus groups were segmented by gender, including two mixed-gender groups, I followed Morgan's (1996), as discussed in section 4.3.2, recommended number of groups with four focus groups of each gender, and two mixed-genders.

Regarding the number of participants per focus group, Morgan (1998) suggests that smaller groups will yield better results when the topics are complex or controversial, as may be the case of the risks of data donation. Each focus group comprised between

six and seven participants, as suggested by Morgan (1996), and earlier discussed in section 4.3.2. Additionally, the decision on the number of participants was pragmatic in the sense that six to seven per focus group was suitable in accordance to the available budget.

As argued above, the participants were divided according to their gender, apart from the last two groups where genders were mixed. This decision was based on the fact that privacy is a gendered issue, and, thus, different genders may construct the risks of donating their data to a smart city project differently (see Tifferet, 2019; Ball et al., 2012; Friedman et al., 2006; Allen 1988; Allen, 1999). For example, in a study by Friedman and colleagues (2006), it was found that generally women expressed more concerns, than men, over being monitored. The authors argue that women feel more vulnerable, especially when it comes to psychological well-being and physical safety. For example, according to the authors, the feeling of being stalked has greater psychological, and, potentially, physical repercussions in women. Ball et al. (2012, pp. 386), exploring how notions of privacy apply to surveillance-intensive workplaces, found that women experience privacy differently. Therefore, when it comes to the study of the constructions of risk in data donation, different genders may have different experiences, and, thus, the need for this study to group participants by gender. Although this research does not aim to look at how different genders construct the risks associated with data donation, this division may prove as a useful tool during the analysis of the data, as well as for forthcoming research articles.

4.4.3.2 VARYING CONDITIONS

The research aims to investigate the construction of risk in the context of mobility data donation. Specifically, how the perception of traditional donation risks, as per Barkworth's framework, interplays with the perception of risks specific to privacy, as per Solove's framework. Therefore, it is necessary to expose the participants to different conditions (vignettes), that, essentially, represent the phenomenon under investigation, in order to elicit the exchange of arguments leading to an understanding of how risk is constructed. It is necessary, however, to argue whether varying the conditions within a group (herein referred to as 'within-group') is a more suitable approach than presenting a different set of conditions between groups (herein referred to as 'between-group').

In a within-group design, the participants may attempt, unconsciously or not, to adapt their arguments to, what they believe to be, the researcher's intentions. This is referred to as the 'demand effect' (Zizzo, 2010). Furthermore, in a within-group design, participants' arguments to the subsequent scenario may be influenced by prior scenarios. This 'carry-over' effect may affect how individuals respond to the scenario in comparison to how they would have discussed it without any prior preconceived idea. This is due to the fact that the subjects feel obliged to adapt their response based on a comparison between the current scenario and the previous scenario (Frederick and Fishchoff, 1998).

Nevertheless, the data gathered from a within-group design does not depend on which group a participant is placed, given that the scenarios will be run similarly in every group. Also, a within-group design gathers a wealth of discursive data that a between-design does not. Participants are observed within multiple situations and their discourses are constantly evolving and adapting from the interaction with others. Therefore, the ‘carry-over effect’ can even be discounted. Lastly, within-group designs are aligned with this research’s theoretical model (Zizzo, 2010): in the real-world, an individual is likely to be facing a set of evolving scenarios surrounding the donation of data that, ultimately, influence their argumentative patterns. For instance, if an individual donates their data but ends up seeing their insurance premium increase, that individual’s response to a subsequent scenario may be different.

In contrast, a between-group design produces data about the discourse of a group facing one condition, and variation of the condition happens between groups. The participants’ argumentative patterns would be dependent on which group they were assigned to. Furthermore, in the case of this research, the interplay between the perceived risks of donation and privacy risks would have to be compared between groups, and between a set of different participants. Whereas, in the case of a within-group design, the researcher may assess the interplay of perceived risks with a set of evolving scenarios and compare it, under the same conditions, to the other groups. Accordingly, the participants construct their discourse based on their own beliefs and constant interaction with others.

4.4.3.3 PROCEDURE

At the beginning of the focus group discussion, the topic of the study and the researcher were introduced. The concept behind smart cities was introduced by using a video where the narrator presented some of the features and use-cases akin to smart cities⁴⁰. This video was shown only until the 1.20-minute mark as not to allow the individuals to have their opinions affected by the way the narrator talks about Smart Cities – mainly concerning their potential benefits, instead of risks. After, participants were asked to introduce themselves, and answer a few basic questions regarding their bicycle and smartphone use as a warm-up task. These questions were devised with the objective of allowing the participants to get acquainted and for them to begin feeling comfortable engaging with each other. Next, a set of transitioning questions were asked regarding their use of community-based participatory mobility apps, such as, for example, the popular Google-owned traffic application Waze. These apps are similar to those existing in smart city projects, in that they ask users to give their mobility data, such as their route and speed, and provide the council, or in the case of Waze, the rest of the community, with specific information when and where necessary (e.g., pothole, police activity, speed cameras, traffic flow, etc.). After these questions, the scenarios were introduced, followed by a discussion at the end of each scenario. At the end, while logistics were being performed (e.g., filling incentive receipt acknowledgment) there was time for a small ‘Q&A’ session with the researcher where the participants demonstrated keen interest and curiosity not only by the research

⁴⁰ “What is a Smart City? | CNBC Explains” <https://www.youtube.com/watch?v=bANfnYDTzxE>

taking place, but also by engaging in a critical discussion regarding the future of privacy, surveillance, and their potential role, as citizens, on a smart city.

A pilot test of the focus groups procedure was conducted with the researcher's family and friends. Two separate groups of six people each were guided through the intended focus groups procedure with no issues being raised throughout. The video used to introduce the participants to the concept of a smart city was said to be very clear, and interesting and did not skew the participants' opinions of smart cities.

4.5 DATA ANALYSIS METHODOLOGY AND METHODS

In this section, the data analysis methodology and methods are presented and discussed. The data collection and analysis methods employed in this study, derived from the ontological and epistemological philosophies adopted and were chosen and adapted in order to support the exploration of the phenomenon studied. This study employed a thematic analysis of the focus groups data. This data was closely examined, coded and re-coded multiple times, in trying to identify common patterns (i.e., themes) being discussed. Once the themes were established, the text coded within those themes was analysed to reveal the social constructions of data donation risk. This section explores the theory surrounding thematic analysis and how this research employed it in order to examine the wealth of qualitative data collected during the focus groups.

4.5.1 THEMATIC ANALYSIS

To explore the themes encompassing the construction of the risk associated with the donation of personal data to a smart city, a thematic analysis was conducted. This analysis focused on identifying arguments related to the two different frameworks in study – traditional donation risk perception dimensions and privacy-specific harms – in search for meaningful patterns that address the research question. The reasoning behind the choice of thematic analysis as the method employed in this research is explained throughout this section together with a brief discussion of what thematic analysis entails and the steps followed to produce reliable results.

Thematic analysis is a well-established method both in risk research (e.g., Lohiniva et al., 2020; Lee, Ayers, and Holden, 2016), privacy research (e.g., Becker et al., 2017; Sayre and Horne, 2000), and in donation research (Smith, Matthews and Fiddler, 2013; Manuel, Solberg and MacDonald, 2010). It is a method often employed due not only to its flexibility and simplicity, but also because it is effective in uncovering patterns within complex data corpus and data sets. Accordingly, it is the method chosen by the author to address the research problem. As this is an abductive research aiming to investigate how individuals understand the risk involved in donating their personal data, the focus on understanding patterns of risk and how they are constructed by the participants is essential. Therefore, the value of thematic analysis as the stand-alone method employed in this research lies in its ability to facilitate the compilation of key topics and characteristics of a large data set, thus allowing for an observation of

patterns and, subsequently, an easier production of a clear and well organised thesis (King, 2004).

There is a disagreement about whether thematic analysis is a stand-alone analytical method. Some authors contend that thematic analysis should be viewed as a tool that assists different qualitative methods (e.g., Holloway and Todres, 2003; Ryan and Bernard, 2000) and not as a method in its own right as other authors argue (e.g., King, 2004; Braun and Clarke, 2006). It pertains to the fact that since thematic analysis is widely used across different qualitative methods many consider it a process or a supporting tool, rather than a method (Nowell et al., 2017). This research, in accordance with Nowell et al. (2017), King (2004), Braun and Clarke (2006), and others, adopts thematic analysis as the sole method of analysing the qualitative data generated by the focus groups. The reason for this stance is that I agree with these former authors who argued for the use of thematic analysis as a “highly flexible approach that can be modified for the needs of many studies, providing a rich and detailed, yet complex account of data” (Nowell et al., 2017, pp. 2).

Thematic analysis is a method that allows for the organisation, identification, analysis, and reporting of themes observed within a qualitative data set with the objective of finding repeated patterns of meaning (Braun and Clarke, 2006; Nowell et al., 2017). The researcher, by understanding the data set, aims to uncover themes within different pieces of data – in the case of this research: participants’ arguments. These themes are, at a first instance, codes that the researcher attributes to pieces of text. These codes, as Braun and Clarke (ibid) argue, are fluid in that they are constantly evolving and

changing as the process evolves. The objective is that, at the end of the analysis, the researcher is able to report observed patterns of meaning and is able to explain how they were present in that data. However, one of the struggles with this method is that there is no clear-cut way of applying it, as is the case with other qualitative methods, and thus the reliability of the findings is open to interpretation often leading to disagreements between readers (Nowell et al., 2017). Accordingly, in order to ensure the reliability of this analysis, and to provide the reader with information as to how the researcher analysed the data corpus, this research adopts Braun and Clarke's (2006) framework, and their proposed 'six phases of thematic analysis'.

Braun and Clarke (2006) start by proposing that the researcher familiarises themselves with the data collected. An immersive, repeated and active readings of the data familiarises the researcher with the extent and depth of the data. This usually entails at least one thorough reading with several notes taken, including some ideas for possible codes.

Once the researcher is familiar with the data, the next step pertains to the generation of the initial codes. Bearing in mind that these will be subject to several revisions as the analysis process continues, the initial coding provides the researcher with an organisation of raw data into relevant groups (Tuckett, 2005). This step is dependent on how the researcher approaches the analysis. If the research is more 'data-driven' the researcher will look for codes independent of their own or others' theoretical position. Conversely, if the research is more 'theory-driven', the researcher may look at the data with specific questions in mind. In the case of this research, as it is detailed

in the section below, the initial coding structure was designed around the frameworks in study and with some questions in mind pertaining. However, the coding was not locked onto this structure and it often changed even throughout this initial step.

The third phase pertains to the search for themes in the previously identified codes. In this phase, the researcher examines how different codes may interplay to represent themes and sub-themes. In this phase some visual representations may aid the researcher in understanding how codes may relate, although it is not a requirement to produce a reliable analysis.

Phases four and five relate to the review and definition of the themes, respectively. Once the themes are identified, the researcher proceeds to review them in order to ascertain whether there is enough data to support them, whether this data is not too diverse and whether they fit within the overall context of the research (i.e., whether they are meaningful). This review may result in themes being separated in two, collapsed in to one, or simply discarded. After the remaining themes are identified, it is important for the researcher to read the data set once more to understand how the theme works in relation to the whole data set, and to, if necessary, to add any missing data into the theme. Once this is done, then the researcher moves on to define the themes identified. This entails a written note of what each theme is about and how does it fit into the overall topic in study.

Lastly, to conclude the analysis, the researcher writes a report where the story of those themes is told in the context of the study. It is essential that the report convinces the

reader of the merit and validity of the research. These six steps ensure the consistency and reliability of the research and allow for a comprehensive search for patterns of meanings within the data set analysed. Furthermore, it provides the reader with confidence that, despite the largely interpretative essence of this study, the results achieved are reliable.

Thematic Analysis, however, has a few disadvantages. The most striking shortcoming of this method is the lack of rich literature when comparing to other methods, such as, for example, ethnography. Accordingly, performing thematic analysis without the due support of a substantial body of research may feel complex, especially for an early career researcher (Nowell et al., 2017). Furthermore, one of thematic analysis' advantage - its flexibility - can also be a disadvantage when compared to other qualitative methods. This flexibility can contribute to a certain discrepancy and lack of consistency in the results of the analysis (Holloway and Todres, 2003). However, as they argue, this potential lack of consistency and discrepancy in themes can be mitigated by making clear the epistemological position guiding the research. This will heavily influence the way results are interpreted and themes derived.

Accordingly, the researcher addresses these shortcomings by relying predominantly on Braun and Clarke's (2006) framework to conduct thematic analysis and ascertain the reliability of its results. Furthermore, the researcher, at the beginning of this chapter argued for his ontological and epistemological positions that guide the analysis of the data sets. The next section goes into further detail on how the researcher analysed the data.

4.5.2 DOING THEMATIC ANALYSIS

After discussing and arguing for the employment of thematic analysis in this research, this section proceeds to demonstrate how the data was analysed in order to produce the results discussed in chapter six.

The focus groups audio data was transcribed by an agency, previously vetted by the University of St Andrews. The transcription files were then imported to NVivo 11, a software programme where the manual ascription of codes and analysis took place. The coding, and eventual analysis, of the data was organised around two frameworks: the traditional risk framework, discussed in chapter two; and the privacy-specific framework discussed in chapter three. While the first topic focuses on the risks more broadly perceived, specifically in the context of traditional donation practices, the second focused on risk specific to privacy. Despite the fact that there were no pre-fixed codes, these frameworks provided the basis for an early coding structure. Therefore, after two thorough readings without any preconceptions of where themes may lie, codes were assigned depending on whether arguments identified, intensified or mitigated a given risk. If a risk was identified or intensified, then a code was assigned based on the framework in study it represented. Conversely, if the data pertained to a mitigatory argument, then a code would be assigned according to the situation depicted. This, however, was being based on any framework as these focus solely on risk and not in its mitigation. While coding and re-coding with every iteration of the reading, the researcher started writing the analysis chapter in order to better understand possible patterns and interplays. Once themes and patterns of meaning were evident,

the data was once more reviewed in search for missing codes and inconsistencies while the report was being devised. The final coding tree is in appendix 4.

4.6 ETHICAL CONSIDERATIONS

Considering the ethical issues and implications involved in generating knowledge is essential in any research and to every researcher. Ensuring that results are independent from any external influence (e.g., funding bodies), and that the participants' wellbeing and right to consent, confidentiality, and anonymity were central concerns to the researcher is vital.

This research took into consideration three essential ethical issues: consent, confidentiality, and anonymity. First, consent is a key ethical issue in any empirical research using humans as subjects. Consent pertains to the notion of autonomy. In specific, to the process of protecting and supporting the participants' autonomous decision making (Beauchamp, 2009; Sim and Waterfield, 2019). In other words, consent is vital as it allows the individual to make an informed decision to participate in the research after carefully considering all the information related to the focus groups that the researcher makes available, free from coercion. It is especially important in focus groups research as participants not only share their beliefs with the interviewer, or, in this case, moderator, but also disclose them to the other participants (Green and Hart, 1999).

Therefore, seeking the participants' consent was a key ethical step to consider. Accordingly, QRS, the market recruitment company, after identifying the suitable participants and receiving their initial interest in partaking in the research, a participant information sheet (PIS) was distributed. This PIS gave key information about the research, how the focus groups would be conducted, and what would be expected from their participation. Specifically, information regarding what the study is about, the risks the participants could face, who is funding the study, what type of data and how it will be collected, stored, used, and shared, amongst other things were presented. All this information is vital so that the participants can give their informed consent prior to the focus groups taking place.

Between agreeing to participate in the focus groups and the date of their participation, individuals had the chance to digest the information given in the PIS, as well as e-mail the researcher with any questions they may have had. On the day of their focus groups interviews, prior to the beginning of the discussion, every participant was given the opportunity to ask questions. Furthermore, a quick briefing of what was expected was discussed before asking the participants to read and sign a consent sheet. By allowing as much time as possible and by providing a wealth of information regarding the study and their participation, the researcher ensured that informed consent would be given.

Consent is often regarded as revocable (Faden and Beauchamp, 1986). Accordingly, in the consent form provided, participants were told that they could revoke their consent to participate at any point without the need to provide any explanation. However, this may prove challenging in a focus group setting. Contrary to, for

example, an in-depth interview, withdrawing consent in the middle of a group discussion may be challenging. First, “withdrawing from a focus groups discussion is a very public and potentially disruptive act that an individual may find hard to perform” (Sim and Waterfield, 2019, pp. 3006). Second, once the discussion, and its digital recording, starts the participants are anonymised.

In other words, the audio material that will be transcribed does not contain any personal identifiable information, unless the participants disclose it during the discussion – which the researcher strongly advises against during the initial briefing. Nonetheless, if this is the case, during the transcription, anonymous coding would be attributed to that information, so as to guarantee the safety and anonymity of the participants. Accordingly, withdrawing consent at any point after the discussion starts is very challenging. Participants are free to leave at any point during the discussion. However, the data they provided, the arguments they put forward previously could not be removed from the transcripts. Doing so would put the integrity and reliability of the analysis in jeopardy. As Sim and Waterfield (2019, pp. 3007) put it: “the analytic insights that emerge are co-constructed by all the participants, and indeed the moderator also. Thus, the removal of a section of dialogue may make it hard, or even impossible, to meaningfully interpret subsequent dialogue”. Participants were so informed that they are free to withdraw their consent at any point, however, once the data is anonymised, it would be impossible to remove it.

It is equally important to discuss how confidentiality and anonymity were assured. Confidentiality refers to how the researcher manages the information once it is in their

possession. In specific, how and to what extent is it disclosed to others. Anonymity, another key ethical issue, refers to the identification of information. In other words, whether participants can be identified from the information held by the researcher. “An obvious way to preserve anonymity is to ensure that no real names or other directly identifying information are reported” (Sim and Waterfield, 2019, pp. 3009). Accordingly, participants were instructed to refrain from using any identifiable information once the recording started, instead they were asked to, at the beginning, introduce themselves as ‘participant number x’. This way, when transcribing the audio recordings, it would be easier to attribute an argument to a participant while ensuring their anonymity. Should they discuss some personal information during the focus groups, this would be anonymised during transcription. For example, if someone argues that “My mom always said, X you need to think before opening your mouth”, or “Where I live, by the stadium on X street, there are a lot of bikes passing every day”, the transcription company was instructed to change the personal details with a “P”, to be understood as a reference to the fact that it was a participant arguing that and, if the information disclosed does not relate to the participant’s name, the transcription company will enter a “=” before and after the sensitive data.

All audio recordings were destroyed once transcribed. The now anonymised data guarantees that no-one, including the researchers, could use any reasonably available means to identify participants from the data. The anonymised data was stored in an encrypted and backed-up external hard drive, and only the researcher, supervisors, and a third-party company in charge of transcribing the focus group data were able to access it.

The only personal data collected were the participants' names and surnames, that allowed them to sign into the focus group, and, inevitably, their city of residence. These data, however, were kept separate from any data pertaining to the focus group discussion (i.e., data that would be transcribed and analysed) and destroyed immediately after the focus group takes place. The audio recordings were kept securely and stored separately to any identifiable information (e.g., consent forms). This way, both confidentiality and anonymity were assured. At the end of the focus groups, the participants were debriefed, and given a debrief sheet with all the information pertaining to how their confidentiality and anonymity are assured.

Furthermore, the scenarios employed in the different focus groups ask the participants discuss a potential decision: to donate or not personal data. However, this particular task may be sensitive to some participants as the scenarios portrayed could prove quite personal, especially if they had their personal data misused in the past. This potential psychological harm was addressed by presenting and discussing the vignettes around a fictitious character, Kris. This way, participants will be discussing what should the character do and the reasoning behind that decision, instead of diving into details of their personal lives.

Lastly, in order to ensure that this research is inclusive, the physical spaces at the location where the fieldwork takes place (The Open University), are accessible by disabled people, and adjustments will be made to participants who may require them. Besides the issues explored above, no further ethical issues are expected. The University of St Andrew's School of Management Ethics Committee approved the

application (Ethics Authorisation number MN14450). The ethics authorisation, ethics application form, consent form, participant information sheet, and debriefing sheet can be consulted in appendices 5, 6, 7, 8, and 9 respectively.

4.7 CONCLUSION

In this chapter the ontological and epistemological positions of the researcher were discussed together with the methodology and methods employed to address the research question proposed. Specifically, the suitability of the social constructionist philosophical position of the researcher was explored.

Following key informant interviews, a within group qualitative study was described, which used focus groups as its main data collection method. Vignettes about data collection were used as stimulus material. A total of 61 people participated divided along ten focus groups. Participants were, on average 40 years old, split evenly amongst genders and the results of this analysis are now described in chapter five.

Chapter 5: RESULTS CHAPTER

5.1 INTRODUCTION

This chapter presents and explores the results of the study. It does so by addressing the way the data was coded and by exploring the issues raised by the participants in the way they framed their argumentation. It presents the first two phases of a three-phase thematic analysis. In the first phase of thematic analysis, all discussion relating to the risks involved in data donation were identified. Participants expressed these risks by exploring reasons why they would be concerned about donating data. In the second phase of the thematic analysis, the risks discussed were classified according to an a priori set of codes derived from the theoretical frameworks explained in chapters 2 and 3. The a priori codebook formed a comprehensive thematic basis through which these arguments were classified and understood.

Alongside the discussion of risks, participants also discussed reasons why they would donate data. These discussions are also thematically analysed in this chapter. Although the a priori codebook was not applied and these discussions were coded on an emergent basis, it was found that the constructed themes mapped very closely on to the a priori codes derived from the donation literature.

The results of the first two phases of analysis are presented in the chapter. It is concluded that two types of arguments were being made: those which reinforced the risks associated with data donation, making it less attractive for the participants, and those which mitigated the risks associated with data donation, making it more attractive to the participants. The thematic basis of these arguments which reinforce and mitigate data donation risk appears to lie within the traditional donation framework. There also appears to be interplay between the privacy and donation risks. Representing the third phase of analysis, the thematic relationship between privacy risks and traditional donation risks is analysed further and presented in chapter six in order to answer the research question.

Furthermore, it is worth noting that the lens of data donation was not one that the participants of the focus groups were acquainted with. Although a detailed explanation of what data donation entails and how it is different from data sharing was provided prior to the start of the discussion, participants still blurred the line between both by often referring to, and moving the discussion to, data sharing instead of data donation. In light of this, the researcher had to constantly remind the participants of the difference throughout the discussion, often asking them what they meant by ‘giving their data’ or ‘sharing their data’ in order to understand whether it would be aligned with the topic being researched. With these interventions, the researcher tried to ensure an appropriate flow and context of the discussion.

This chapter is structured as follows. First, a brief introduction is given to the focus group participants and process. Then the first and second phases of analysis are

presented, representing a classification of the risks identified by the focus group participants in their talk according to the a priori codes. Then, a thematic analysis of the reasons in favour of data donation are presented before conclusions are drawn.

The ten focus groups were conducted from 6 PM to 8 PM for a total of five working days (Monday to Friday). One hour was allocated to each group discussion and, in general, everyone was punctual with each focus group lasting, on average, 50 minutes. Furthermore, only two individuals failed to attend. Every focus group had between six and seven participants, for a total of 61 participants – 30 male participants and 31 female participants.

The average age was 40.7 years old, with the most common being 35 years old. The majority of the participants cycle once or twice per week (33 participants), followed by more than twice but not every day (16 participants). Moreover, the average cycling journey time is 39.66 minutes, with the most common journey time being 25 minutes.

The table below summarises these statistics:

Average Age	Mode Age	How often do you cycle? - Mode	Average Journey Time	Mode Journey Time
40.7 Years Old	35 Years Old	Once or Twice per week (54 % of the participants)	39.66 minutes	25 minutes

Table 4 - Focus Groups Statistics

5.2 INTRODUCTORY QUESTIONS

Before introducing the scenarios, a few ice-breaking questions were asked. First, when asked how they would define the term ‘smart city’ the participants’ answers were quite scattered and there was never an apparent consensus in any of the focus groups. Responses ranged from “it’s monitoring you all the time” (P4, FG5), or “trying to influence you to buy something” (P5, FG5), to “a city that doesn’t really have people driving around the city. Mainly just walking, smart cars, sort of thing, biking to work.” (P1, FG6). Nonetheless, despite these contrasting opinions, the term ‘smart city’ raises notions of technology being used for different purposes – this was the common denominator across the attempts to explain the term. The variation is in the purpose of this technology - to surveil, control the population, become sustainable, become efficient, or to simply aid the population’s mobility. The rest of the questions asked, were for the sole purpose of getting the participants acquainted and at ease with engaging in a discussion with their peers. The section below now turns the attention to the dynamics within the focus groups discussions.

5.3 THE DYNAMICS WITHIN THE FOCUS GROUPS

As focus groups involve several people in a discussion setting, promoting the interaction between them and the exchange of arguments, different dynamics between the different focus groups were observed. As the researcher adopted a social constructionist stance, this topic is of particular importance to be addressed since the

different dynamics may have had an impact in shaping the participants' constructions of risk.

As with any other group interview, having more than one participant engaging in a discussion makes it that one or a couple of individuals take a more dominant dynamic in the conversation and general interaction with the other members. Throughout the focus groups conducted for this research this was not any different. In every focus group there was at least one individual who looked to dominate the discussion and influence others' opinions. Interestingly, in the two mixed-gender groups, females tended to be the ones voicing their opinions and experiences more strongly than their male counterparts. This power differential and dynamic influenced how the risk of donating personal data to a smart city was being socially constructed by the participants. Although explaining how this power asymmetry influenced the constructions of risk is not the focus of this research, it is important to acknowledge its importance and influence on the risk construction process.

Furthermore, although in some focus groups conducted by other researchers (e.g., Farnsworth and Boon, 2010), hostility amongst participants has been reported, there has been no hostility observed during this research's focus groups. On the contrary, participants seemed to form bonds between them, often exchanging contact information at the end of the discussion and inviting one another for a coffee or a dinner at a local restaurant close to the location. Throughout the discussion, participants seemed to identify with one another, likely linking to the idea of social identity previously discussed in chapter three. Participants might have been from

different socioeconomic backgrounds, but all shared (at least) one key psychographic characteristic: they were all passionate about cycling, thus forming a sense of community that tends to be a remarkable characteristic of this social group (e.g., Hoekstra, Twisk, and Hagenzieker, 2018).

The dynamics here identified, together with other presents (e.g., different socioeconomic backgrounds and socioeconomic disparity – a professor of computer science was present in the same focus group as an unemployed participant) might have had an influence on the outcomes of the discussion. One person may be more aware of technology and issues surrounding it in smart cities (e.g., professor of computer science) whereas other people could offer a more family centric voice based on their experience with applications and other smart city technologies (e.g., unemployed participant). Nonetheless, even though I acknowledge the impact these dynamics may have had on the results of the discussions, these are somewhat hard to assess given that my focus was on the interplay of arguments in the discussion and not on how the different dynamics influence the results.

The next section explores the concerns participants voiced with donating their personal data to a smart city project. Especially, when it comes to identifying and reinforcing the risks to their peers during the focus groups discussions.

5.4 CONCERNS WITH DATA DONATION: IDENTIFYING AND REINFORCING THE RISKS

This section discusses the codes referring to the identification and reinforcement of the risks discussed by the focus groups participants. It provides data from the focus groups discussions to support the codes ascribed. Data were first coded using a set of a priori codes derived from the risk frameworks advanced by Solove and Barkworth. Codes pertaining to data collection, processing, dissemination and privacy invasion, as well as codes pertaining to physical, psychological, social, financial, time, and performance constructed risks feature in the first instance.

The table below presents the different codes identified in the participants' arguments, as per the risk frameworks explored. Furthermore, it also displays the number of references a certain risk was coded, and in how many focus groups that risk was discussed. The most frequently cited concern relates to how the participants' personal data is collected by the smart city project.

Codes	N Focus Groups	N References Coded
Data Collection	9	122
Data Processing	8	78
Data Dissemination	9	90
Invasion	7	23
Physical Safety	8	32
Financial	9	31
Psychological	10	75
Time	10	56
Social	5	7
Performance	7	28

Table 5 - Summary of Nodes Coded and Their Frequency

5.4.1 DATA COLLECTION RISKS

Arguments pertaining to data collection as a potential risk to data donation were coded 122 times. These risks were amongst the most frequently argued during the focus groups discussions. Participants reflected on how they would react if faced with the opportunity to donate personal data. From this, a concern about data collection was created and the risk seemed to be constructed out of a concern for the amount of data collected, the breadth of data, and the trustworthiness of the third party that was collecting their data.

The following quote from focus group 10 in response to the second scenario, where the city council provides a fitness tracker in exchange for heart rate and weight data, exhibits a clear concern for the amount of data that is collected. Another participant soon followed by summarizing the previous argument by claiming “a bit too personal I think”. Interestingly, the participant culminated by arguing “yea ok I’m fat, ..., don’t have to tell you about it every day”. This notes a potential judgement regarding the physical features of the self that the participant may be conscious about and is not comfortable with third parties receiving that personal information.

FP4 – No, what more do they want? Oh my God. They’re gonna want foot size, nose size, hand size, what else size [overtalking]. There’s gotta be a point where you’re gonna have to stop. Like yeah okay I’m fat, that’s, you know, don’t have to tell you about it every day. That’s... I think that’s just plain...

MP1 – A bit too personal I think.

(FG 10)

In the next example, the concern relates to when, and for how long, is the app tracking the participants. The risk participants discuss encompasses the way data is being collected. The data collection risk here identified is not immediately dismissed, but is reinforced by others that, perhaps, have not yet considered it. For example, when participant six interjects with a “oh, oh that’s not good”.

P4 – What about driving as well? If you're driving a car and you speed, it's got all your speeding [laughs], it's got your speeding as well.

P1 – Yes, I was going to say is it recording [overtalking] all, all the time, then?

P6 – Oh, oh that's not good [laughter].

P1 – Is it all, all the time? So, it's not whether you're cycling or not, it's just all the time?

(FG 5)

These previous examples represent the constructions of risk relating to how the participants' information is collected by the city council. Namely, the type of information collected, when is it collected, and whether they trust the city council with their personal information.

5.4.2 DATA PROCESSING

Concerns regarding the way data is processed by the third parties were coded 78 times. Arguments pertaining to the 'data processing category' included participants' concerns related to being excluded from certain services (e.g. NHS services), using their personal data for something to which they did not initially consent, the safety of

their information, and whether the data, that initially they thought it was anonymously donated, could be used to identify them at a later stage.

Two examples that illustrate some of these arguments are now presented. Below, in the first instance, a participant argues about their apprehension regarding the fact that if they donated their data, they might be excluded from certain services. Namely, participant five demonstrates a concern that the donated data may be used to exclude specific people (e.g., smokers, obese people) from NHS services.

P5 – It would make me very suspicious if you think about when we look at the NHS [overtalking] and what they're talking about. How they're talking about sort of reducing certain services for certain people. Whether they're going to be obese or if they're smokers, you're not going to be able to get certain sort of medications for different conditions. I know, I can't help but think that could this data, maybe not now...

P6 – Yes, but in the future.

P5 – Be applied to that sort of thing.

P2 – Mm-hm.

(FG 7)

The risks constructed by the participants relating to the way their data is processed are not always explicitly argued. Some are more vaguely argued. For example, in the excerpt below, participant four, from focus group two, demonstrates a concern regarding how their son's school may process their child's information: "It's, like, they've got his print, and God knows..." With emphasis to the expression: "and God knows" constructing the data processing risk as being based on their sense that they do not know exactly what is done with their personal data.

P4 – Like, my son's school [inhales], a secondary school [tapping sound], they have to finger for lunch. You know, like, you put it on the pad and then it authorises how much is on the account, and they can buy their [sniff] lunch. And that's data collecting, so...

P4 – I don't [finger clicking] know what they'll do with that after...

P3 – At least you know what he [unclear] for lunch.

P3 – What he's had for lunch. [Laughter].

P4 – It's, like, they've got his print, and God knows...

P2 – Yeah.

(FG 2)

5.4.3 DATA DISSEMINATION

Concerns about the possible dissemination of individuals' personal data, by the city council, without their informed consent were coded 90 times. Risks were constructed in this code on the basis of unauthorised disclosure to a third party, exposure, increased accessibility, and the breach of the assumed confidentiality of the programme.

In the example below, participant one, from focus group four, when discussing whether a financial incentive could mitigate the fact that personal data was disseminated to their insurer, the individual argued:

P1 – So I'll, I'll take it a step further and different scenario. I break into your house...

P5 – Yep.

P1 – And I leave you £50 on the kitchen table and say, you're welcome.

P5 – Yep.

P1 – You don't feel good about that.

P5 – No.

P1 – I still did something against your will that you didn't expect. You got some money, but you're still phoning the police. It's the same...

(FG 4)

Therefore, in this particular illustration offered by the participant, the fact that their personal data was disseminated to a third party without their previous represented a clear risk to the participant. The participant argued that even if someone broke into their house to leave some money on the counter, they would not be happy that they entered without previously asking for consent. Data dissemination, disclosure in this case, is clearly a risk perceived by participants.

Other examples are not as specific as the previous one. In the quotation below, the risks constructed by the participants are as vague as demonstrating apprehension regarding to whom will their personal information be passed on.

FP4 – Yeah and if they picked up this data what organisations are they gonna pass it onto?

FP6 – Yeah, sharing his information.

(FG 9)

5.4.4 INVASION

Codes concerning the invasion by a third party into the participant's personal life were the least present in the participants' arguments with 23 arguments coded. Although still a constructed risk, it is articulated much less by the participants. Arguments ascribed with the 'invasion' code were related with intrusion into one's life. For instance, receiving nuisance calls, and spam e-mails may disturb the individual's routine, activities, solitude and peace of mind. Moreover, arguments concerned with the interference in the individual's decisions were equally ascribed the 'invasion' code. For instance, the use of targeted advertisements with the objective of influencing an individual's (or group of individuals) decision (e.g., Cambridge Analytica scandal) is classified as an invasion.

In one specific case of the focus groups discussions, as illustrated in the passage below, the constructed risk identified by participant four is related to pop up advertising from a product called "SlimFast". Specifically, what is the meaning of this kind of advert "popping up" on their social media feed.

***FP4** – There's SlimFast keeps popping up [laughter] and you're like, right, okay, yeah, I've been spied upon here.*

***MP2** – You're thinking, well why has he got that? He must be [overtalking].*

FP4 – Especially as a woman. They could be... Kris is, you know, a woman again. And she's like, oh my goodness, they're giving me advertisements for my weight. Problem which I wasn't aware was a problem. And she was happier with herself.

(FG 10)

In this next example, the participant 'invasion' arguments are illustrated by their use of the word "harassed" when they receive these unwanted calls.

P5 – I think [unclear] you get, um, harassed and get called. And I know they're not allowed to really call you now and keep...

(FG 3)

After discussing the privacy-specific risks of donating personal data to a smart city, the chapter continues by turning the attention towards the categories of the traditional risks of donation and how these were discussed by the focus groups in the context of this research.

5.4.5 PHYSICAL SAFETY

The participants' constructed risks relating to their physical safety were identified in 32 arguments. The responses pertaining to this code included concerns of being stalked, raped, murdered, concern for the wellbeing of their relatives and loved ones, and, in general, whether the information donated could, somehow, put them in any sort of physical danger.

The following examples provide an illustration of some of the arguments used by the participants pertaining to the 'physical safety' code. After the introduction of location-tracking as one of the features of the app, the evolution of the conversation leads to an exchange of arguments relating to the participants' fear for their physical safety. In the particular example below, participant three discusses the fact that if Kris' location is displayed to the public, they could be harmed.

P3 – And who is looking at it? Is it just the people who want to know about the potholes or is it the wider community? Because people will get to know where Kris is at what time. And, if he's in a particularly secluded area, say the Redways around here, some of the parts you could be in could just be bushes and it can be a bit frightening sometimes if you're there on your own. So, if you were always at that point at a certain time, early morning or later on in the evening [overtalking].

P2 – Be in trouble.

P1 – It's a safety thing.

P3 – People would know that [overtalking].

P1 – Put yourself at risk, really.

P5 – And, maybe getting murdered if you're being tracked [laughing] by psychopaths.

(FG 7)

Similarly, in the example below, participant one in focus group six argues that should their personal information be used by “some sick people” then they could be in danger. Participant three reinforces the argument by claiming that they are already aware of this, and thus disable the location tracking on every app they and their family use.

P1 – But on the other hand, there are some sick people out there that will be using that kind of information...

P3 – Well I make sure that myself and my children have completely got location off every single thing that we do...

P1 – Exactly, your location services.

(FG 6)

Lastly, participant two from the focus group two, argues that, if Kris decides to participate in the smart city programme by donating personal data, they “could get stalked” – an argument clearly representing the ‘physical safety’ code.

P2 – He could get stalked.

(FG 2)

5.4.6 FINANCIAL

Arguments pertaining to the constructed financial risks of personal data donation were coded 31 times. The arguments exchanged in the focus groups’ discussions included in this code encompass a potential rise in insurance premiums and even robberies should they decide to donate their personal data. These arguments denote a clear impact for the individual’s financial wellbeing. The examples below illustrate these arguments. For instance, participants often referred to the financial implications of having their personal data passed on to insurance companies (e.g. rise in premiums). It differs from perceived risks of dissemination, as argued above, because the participants accentuate their argumentation on the financial consequences of such

dissemination. In several focus groups it was argued that if sensitive data (e.g. weight) was eventually disclosed to an insurance company it would certainly lead to an increase in the premium. This interplay is further explored in the next chapter.

P6 – For example, if it was passed on to insurance companies, like life insurance, then that could affect your own life insurance cover.

(FG 1)

P1 – If Kris has got no health issues, I don't think it's a problem. But if he's overweight [sniff], his insurance might be affected or something...

(FG 2)

P2 – What, what you've described is such a serious breach because it's impacted him financially.

P1 – Yes. Yes.

P2 – Once you impact people financially, people's backs really get up.

(FG 4)

Furthermore, another argument concerning financial implications is related to the fact that disclosure of location data may lead to robberies. Again, although the participant

clearly perceives a data dissemination risk, it accentuates the argument on its perceived financial risk. In other words, and adopting the example illustrated below by participant three of focus group seven, they may have their bicycle stolen if someone knows where they store it overnight.

P3 - I used to be a member of a cycling group just up the road. And, they had tracked on Strava or one of these other apps what type of bike they had, how old it was, when they changed their tires to new ones. When they did this, this and this. And, he had an expensive bike. And, somebody followed him on Strava and pin-pointed his address and stole the bike from the garage.

P2 - You see?

(FG 7)

5.4.7 PSYCHOLOGICAL

Psychological impacts of data donation were mentioned 75 times. Constructed psychological risks are expressed slightly more subtly than the previous financial risk. This is due to the fact that, for participants, it is harder to explicitly construct psychological risks. Especially because they are not directly asked what type of risks they are constructing; thus, this understanding is derived through analysis of the arguments exchanged. Accordingly, arguments were re-interpreted in a way which

brought mental wellbeing aspects of the argument to the fore. Arguments ascribed this code included the possibility of being stalked, as a constructed psychological as well as a physical wellbeing risk, ‘feeling judged’, feeling of pressure to lose weight, or the feeling of unease regarding the fact that others may have access to such personal data (e.g., about health and fitness levels). The quotation below illustrates a feeling of judgement regarding Kris’ cycling performance and fitness levels: “he could feel judged”. This feeling undoubtedly constructs a psychological risk.

P3 – If he were feeling cynical, he could feel judged on his performance.

P3 – Do you know what I mean? If he, if that day he is going out there, you could almost feel the pressure on that performance, do you know what I mean? Dependent on how keen he is, or how, um, competitive he is. But he might think, oh I might all of a sudden be judged by people.

P2 – I think that’s where the human side comes into it, isn’t it? So yeah, some of it definitely gonna feel that way. Whereas some people gonna feel special because they’ve been invited, so, yeah.

(FG 4)

Similarly, the passage below sees an individual arguing that participating in this smart city project “might shame Kris to lose weight”. This argument, in special the

employment of the expression ‘shame him’, depicts an apparent constructed psychological risk of donating personal data.

P6 –It might shame Kris to lose weight [laughing].

P2 –Yes, but then don’t you think, um, now you’re putting your weight and then there’s somebody who’s expecting you to lose that weight. What if...? You know [overtalking], there’s some diets that you go on and you don’t even lose anything, you just keep eating your rabbit for two weeks.

(FG 7)

Lastly, in the example below, of participant one of focus group two, their discussion constructs the risk of being stalked should someone have access to their personal information on Strava (an application, and social network, that allows users to track their physical activity, connect to their friends, and share their information with their network).

P1 – As soon as you started talking about it, I thought, yes, someone could stalk me on Strava.

(FG 2)

5.4.8 TIME

The ‘time’ code was ascribed 56 times. This code included arguments that donating personal data would somehow create an annoyance or disturbance in the individual’s personal routine, that donating data is a time-consuming process, and that they would not have enough knowledge or willingness to engage with the smart city project. For instance, below, participant six, from focus group ten, argues that if the city council asks Kris to stop every time to, for example, report a pothole on the cycling path, then they are just not “gonna [sic] keep stopping”. Adding that if Kris “could do it at a later time...” then perhaps they would be more inclined to donate their data. Clearly, the waste of time, and the disturbance of Kris’ cycling routine, is perceived by the participant as a risk.

P6 – If you travel every day that way, surely he could report it when he got to work or at another time, or not? Would you have to do it there and then?

I – Would that impact your decision?

F6 – Well, yeah, because if he’s finding things on the way all the time, I mean, you’re not gonna keep stopping.

F6 – But if he could do it at a later time...

(FG 10)

Similarly, the following two examples illustrate a constructed time risk of participating in the smart city project. Participant three from focus group two claims that they would not want to stop on their way back from work, perhaps because they are tired, just want to get home faster, or just simply because they do not feel like getting disturbed. In contrast, participant one from focus group six claims that Kris, on their way back from work, may be inclined to stop and report the potholes. However, not while they are commuting to work due to the fact that Kris needs to “get to the office at a certain time, he’s going to have no time”. Contrasting arguments that portray the same perceived time risk.

P3 Wouldn't wanna stop on my way to work

(FG 2)

P1 – On his way back home, yes maybe. But on his way to work which is already 40 minutes and he's got to get to the office at a certain time, he's going to have no time...

(FG 6)

5.4.9 SOCIAL

Constructed risks regarding social implications of donating personal data were coded 7 times. Constructed social risks are those that may have an impact to an individual's social status. Arguments related with this code included concerns regarding someone else having access to and knowing details about one's personal situation. Furthermore, the possibility of consequences deriving from someone else (e.g., wife) accessing that information is another instance of an argument pertaining to this code. As exemplified by the focus groups quotations below, participants were concerned about what would their loved ones think of them if they had access to some given information. Whether it is the fact that their loved ones become aware that they are buying a gift for them, or the fact that they know something that was meant to be kept secret, the argument in these examples constructs a social risk. Participant four of the focus group ten argues that "if he's buying a secret present for the wife [...] you're being tagged". In other words, a risk to an individual's relationship with his wife, part of his family, is constructed if she became aware of his actions through the information he may have donated.

FP4 – If he's buying a secret present for the wife, or somebody, that again, that's giving the game away. You're being tagged.

MP3 – Well, hopefully the wife won't see this information, right?

MP5 – Yeah [laughter].

(FG 10)

In the example below, participant one and six of focus group seven discuss the implications of technology in the specific context of their marriage. “I don’t want my husband looking me up and seeing where I am”; “He used to be like why are you in Costa again?”; and “why are you out clothes shopping?”. Based on their personal experiences, this exchange portrays a judgement by the participants’ husbands should they have access to their information. Accordingly, it constructs a social risk.

P1 – I deliberately have it on my son’s, but he knows about [overtalking].

P6 – I want to have it on my son’s when he goes. But, you know, I don’t want my husband looking me up and seeing where I am.

P1 – Oh, it’s terrible. He used to be like why are you in Costa again? [Laughing].

P6 – Yes, people are like, why are you out clothes shopping? No, I’m not. You are in Next. What? [Unclear] I’m fine. [Laughs].

(FG 7)

5.4.10 PERFORMANCE

Participants constructed performance risks based on ideas about how third parties collected and processed their data. These elements were coded 28 times. This category was especially hard to code as it often resembles other privacy-specific risks. Nonetheless, the arguments ascribed with the ‘performance’ code demonstrate concern over the city council’s performance in the smart city project. It includes arguments related to breach of trust, mishandling of their personal information, and being responsible for whatever consequences derive from the mishandling of personal data. For example, the quotes below show a clear concern of how the institution collection and processing the data handles the participants private information. If they disclose it, the participants “would be very cross”, and “calling customer services”. In other instances, just the concern of how the institution is collecting the data and using it also reveals a perceived risk relating to performance.

P4 – Then we all would, that’s something that I personally would be very cross about and I wouldn’t just be, um, not using the app. I would be calling customer services...

P1 – Oh yes.

P3 – Yes.

P4 – To get that 40 quid back off...

P1 – Yes.

P4 – I would be completely screwing at them to say, you're paying my car insurance excess [laughter].

P2 – Yes, yes [laughter].

(FG 6)

P1 – If I was Kris I would want to make sure that the app wasn't monitoring me when I wasn't doing my commute. So, it's all well and good me agreeing to do the commute and be monitored for the elevation and the speed, etc., etc. But then, once I've got to work and I'm going about my business, so I don't want that app sitting in the background going now I'm watching you [laughing]. I want to be able [overtalking].

(FG 7)

Having discussed the codes ascribed to arguments pertaining to risk identification and reinforcement, the section below discusses the codes attributed to the arguments for donation.

5.5 ARGUMENTS FOR DONATION: MITIGATING THE RISKS?

Now attention is turned towards arguments made in favour of data donation. These were the arguments that either made data donation acceptable to the participants or that alleviated the risks previously identified and reinforced by other participants. Participants' talk was coded thematically as different arguments for donation were constructed. After reflecting on these themes, it appeared that they mapped on to the categories used by Barkworth and colleagues (2002). This observation suggested that risk mitigation was an important part of the argumentation. This is explored in this section.

Codes	N Focus Groups	N References Coded
Avoidance of Physical Dangers	10	58
Financial Benefits	10	132
Psychological Mitigation	9	33
Improving Life / Saving Time	8	80
Social	5	5
Performance	9	60

Table 6 - Summary of Nodes Coded and Their Frequency

5.5.1 AVOIDANCE OF PHYSICAL DANGERS

The code ‘avoidance of physical dangers’ was ascribed 58 times. This code included arguments pertaining to the use of apps that allow the participants to monitor their loved ones as means to guarantee their safety. Namely, the use of these technologies to monitor where their children are, if their partner has an accident, to be reassured that everything is fine.

It was previously discussed that participants intensified the risks of data donation partly by constructing risks to their physical safety. Conversely, arguments concerning physical safety were also used to mitigate risks of donating personal data. For instance, in the example below from focus group two, participant one offered an example of how an app’s location tracking feature helped saving her friend’s husband from a biking accident: “[he] had a really bad accident. And it was only because of his [...] smartphone app [...] that his wife was able to find exactly where he was”.

P1 – I, I, I, my husband’s [sniff] friend, um, [mouth sound] he last year [inhales], he was on his bike [sniff], um, and he came off the bike, had a really bad accident. [Inhales]. And it was only because of his, the app, the smartphone app [sniff]...The notification [inhales] that his wife was able to find exactly where he was.

P2 – Oh wow.

P1 – He'd come over the top of the handlebars... [Sniff] and sincerely done a lot of damage to his skull. He ended up in John Radcliffe in, um, the hospital...

P2 – Oxford.

P1 – Oxford, yes. [Inhales]. And that was because of the smartphone and the app. Because she could see that he hadn't moved. [Inhales].

(FG 2)

Another example discussed in focus group six is the use of the app: *Life360*⁴¹. This app allows its users to track a plethora of data from their loved ones. Participant three from focus group six illustrates how they use this app to track their children's daily activities. Namely, when they arrive to school, when they get back home, how much battery is left on their phone, where they are at any given moment, amongst other types of information. The participant claimed that, despite their children's unease with being monitored, it is "about you being safe and me being safe [...] I am just using it for you to be safe". Participant one immediately concurred: "Yes that's all that matters, yes".

P3 – But when he brought it up. He said, I said look I don't care about what you feel. I said this is about you being safe and me being safe...

⁴¹ www.life360.com

P1 – Yes that's all that matters, yes.

*P3 – And that's all that matters. I said I'm not using it to sort of tell you off...
I'm just using it for you to be safe.*

*P3 – So I know that my son, left, left home at like, he left school at 3:27, and
I'm at work. But he gets home 15 minutes later, and I don't have to worry.*

P1 – And then you know when he's at home, yes.

(FG 6)

Lastly, in the example below pertaining to the code being discussed, participant seven of focus group seven questions whether using the app could help Kris should they, for instance, fall off their bicycle: “Is there something in this smart city that could trigger some sort of posse?”

P7 – Because I wonder [overtalking] if something happened to Kris on the way home, he falls off his bike or goes down one of those potholes [laughing] and maybe some safety thing about then he hasn't made it home in a certain time. Is there something in this Smart city then that could trigger some sort of [overtalking] posse?

(FG 7)

5.5.2 FINANCIAL BENEFITS

Mitigatory arguments related to ‘financial benefits’ were coded 132 times. Arguments pertaining to this code include seeking financial benefits in form of discounts, free gadgets, or in-kind payments in exchange for their personal data. Individuals often mitigated risks of donating their data by claiming that they would not mind incurring some risks associated with donating personal information as long as they would receive some form of financial compensation.

For instance, in the example below, participant six, from focus group ten, claims that receiving an insurance letter with an increase in their insurance premium would “annoy them” whilst the contrary, a letter offering them a discount, would make them “happy”. The issue here is not the data being disseminated by the city council to a third party – in this particular case, an insurance company – but the financial implication of that disclosure. Accordingly, as previously argued financial consequences are an argument used to intensify risk, but as now demonstrated, can be an argument used for its mitigation. It all depends on how the individual perceives the outcome of such disclosure.

***FP6** – I was just thinking that a minute ago. If I got the first letter, I’d probably be really annoyed. But, if I got the one...*

***MPI** – You’d be happy, wouldn’t ya?*

FP6 – I dunno, yeah, you'd be happy. You wouldn't complain, would you?

(FG 10)

The exchange below, from focus group two, follows a similar pattern. Participants argue that giving data allows them to receive tailored offers for products they want to buy (i.e., targeted advertising and coupons). In this scenario, giving data, and the potential perceived risks associated, is mitigated by the prospect of receiving, for instance, discount vouchers for products they might be interested in. Accordingly, this argument reflects a mitigation of the risk of giving data by the prospect of some sort of financial return.

P3 – Oh no, it's better for me... I, I used to think that 'cause I used to get so many vouchers that were just irrelevant. And now they only give me vouchers for things I buy.

P2 – Yeah.

P4 – Tailored to what you... Yeah.

P3 – So actually [inhales] a lot of that used to go in the bin, but now...

P3 – It is something I'll use. [Inhales]. So things like that...

P2 – It makes me go back there. There's so many vouchers I'm, like, oh, actually, yeah, that's...

P2 – Everything I use. I'll go [sniff] back there...

P4 – Yeah.

(FG 2)

In this last example, in focus group four, the participants discuss whether they would “get to keep the Fitbit” offered by the city council for the duration of the data donation project. In other words, participants were wondering whether, should they decide to terminate their participation in the data donation programme, they could keep the fitness tracker. Although the scenario does not indicate whether or not the participants get to keep the fitness tracker given by the city for the purposes of the study, they discuss this eventuality as a way to mitigate the risk of giving data. In fact, participant three, from focus group four, even asked whether the city council would offer some perks to the participants, otherwise there would be “no point in doing it at all”. This is another example of the participants arguing for financial benefits in exchange for donating their data to the city council.

P6 – Um, and does he get to keep the Fitbit?

P1 – Yeah that's a good question, do I get to keep the gadget? What's the perk?

[Overtalking]

P2 – [Overtalking] free Fitbit.

P6 – The gadgets. If they're gonna give more for his bike as well.

P3 – Yeah. There's gotta be some perks in it, otherwise it's not... No point in doin' it at all, is there?

(FG 4)

5.5.3 PSYCHOLOGICAL MITIGATION

Psychological mitigatory arguments were coded 33 times. These arguments include the mitigation of the constructed risks constructing some form of psychological benefits from donating (e.g. feeling good for doing good). Moreover, the mitigation of risks as a result of the rationalisation of these same risks (e.g. the 'nothing to hide' argument) were also coded as psychological mitigations.

Arguments pertaining to altruistic motives – 'the warm-glow of giving' as introduced and discussed in chapter two – demonstrate a psychological mitigation of the donation risk. In this case, individuals are rewarded with a positive feeling that is associated

with participating in a charitable action. Also, the infamous ‘nothing to hide’ argument often associated with the dismissal of privacy harms depicts a rationalisation of the risks associated with donating personal data.

Psychological mitigatory arguments, which were built on altruism, were mainly concerned with who the participants’ data was going to benefit. For instance, participants mitigated risks of donating their data constructing the idea that their data could benefit the city and their community. The quote below demonstrates that the participant would be willing to give their personal data to the city council because they are [technically] not a commercial entity. Therefore, the city council ought not to profit from the donated data (i.e. the participants believe that the city council will not sell their personal data), so the individuals do not expect to receive, for example, targeted advertising based on their donated data: “the motive is [...] altruistic in terms of it should be for the benefit of the whole city, rather than a commercial benefit like the other apps that we use” where they expect to receive targeted advertising.

P2 – Well they all follow the same rules, it’s just more like they would be the, not, ‘cause they’re not a commercial kind of organisation, I know they got to, they haven’t got much, much, as much money as what they used to have, but they’re, they have more of a... The motive is, er, is more, sort of, altruistic in terms of it should be for the benefit of the whole city, rather than a commercial benefit like with the other apps that we use. You know, like, I’m expecting to get advertising and expecting to get...

(FG 1)

In the following two examples, participants argue that they would “happily help the community” (P4, FG 6), and that donating their personal data would be a way of “giving back” to said community (P1, FG 4). To these ‘altruistic’ arguments is associated the psychological benefit of ‘feeling good’, as discussed in section 2.4.1.2, the ‘warm glow of giving’.

P4 – If it’s willing, if, ah sorry if it’s voluntary then that’s, that’s [inaudible asides] donation is a good thing the way you word that as a donation...

P1 – Like as a donation, yes.

P4 – Sounds like it’s a willing, um, you know like a, yes, not forced... I Yes.

P6 – Yes, not forced.

P1 – Not forced to do it, yes.

P4 – Yes, I’d happily help the community if that’s what’s going to happen, if there was a big problem.

(FG 6)

P1 – But he might feel he’s doing his best. Well, for the community, as well as for the cycling community. I mean for the community in general. It’s the right path, giving back, isn’t it?

P4 – Mmm.

P1 – Why wouldn’t I provide this data?

(FG 4)

The next example of psychological mitigation is not related with the positive feelings associated with donating personal data. Instead, it is related with the participants argument that data donation would be acceptable for them because they have ‘nothing to hide’. In fact, the ‘nothing to hide’ argument is infamous in surveillance and privacy scholarship for being one of the most argued reasons why individuals so easily dismiss the dangers of privacy-specific risks. In essence, they claim that if someone has nothing to hide, then they should not fear surveillance, as a way to legitimise surveillance practices (see Solove, 2007, 2011; Murumaa-Mengel, Laas-Mikko, and Pruulmann-Vengerfeldt, 2015).

How is this argument a psychological mitigation of risk? Murumaa-Mengel, Laas-Mikko, and Pruulmann-Vengerfeldt (2015, pp. 204) argue that the ‘nothing to hide’ argument stems from the individuals’, and to an extent the population’s, “state of constant stress” derived from the ubiquitous presence of technology in their lives. Even

though the majority of individuals understand that their privacy is being threatened, they have to cope with “an everyday life context in which their information is constantly accessed, collected, and used”. The popular ‘nothing to hide’ argument, although fundamentally flawed, is often used as a coping mechanism. In fact, Murumaa-Mengel, Laas-Mikko, and Pruulmann-Vengerfeldt (2015, pp. 195) calls the ‘nothing to hide’ argument a “coping strategy in a risk society”.

Furthermore, the ‘nothing to hide’ argument can be considered a statement of defiance, and assertion of identity in face of the increasingly invasive surveillance practices: “I am not the person you are looking for” or “I am not the flawed consumer” (Ball, Do Domenico, and Nunan, 2016, pp. 73). Accordingly, the rationalisation that as long as they have nothing to hide, then they should not fear surveillance – and its use as a psychological mitigation argument.

The results of these focus groups were not different: the ‘nothing to hide’ argument was mentioned in six of the ten focus groups conducted and was coded a total of 14 times. The quotations below display some of the arguments used that were ascribed this code. For instance, “people that are law-abiding citizens don’t need to worry about that” or [donating data] “is not good for criminals” were some of the arguments used to mitigate the possible risks of donating personal data.

P7 – People that are law-abiding citizens don’t need to worry about that. Because their, it’s their data that isn’t being, being monitored as such. Well it is, it’s being stored. But it’s not being looked under...

P4 – For any harsh reason or anything, yes.

(FG 3)

P2 – It's not good for criminals.

(FG 8)

P5 – I'm really boring, so I don't think... I don't think I care [overtalking]. My Alexa is probably listening to me permanently [overtalking].

P6 – No, but it's true.

P5 – And all it can hear is me talking to the cats. So, I don't really care. They'll be very bored with me, very quickly.

(FG 7)

5.5.4 IMPROVING LIFE / SAVING TIME

Arguments referring to saving time and improving their life were coded 80 times. These arguments pertain to the individuals' desire to save time during their commute and other daily activities, whether the technology could help improve their lives (e.g.

warn them about traffic conditions, turn on the heating at home remotely, check who rang the doorbell when no one is at home). To these types of arguments, the ‘improving life / saving time’ code was ascribed.

In focus group ten, participant one argues that if donating their personal information by participating in the smart city project improves their commute, then they would be willing to participate. There is a notion of trade-off flowing: participants argue for possible risks they may incurring associated with donating their personal data poised against the possibility for an improvement in their daily lives – most often discussed as saving time commuting. Accordingly, the code ascribed to data depicting this mitigatory argument refers to ‘improvement in daily life’ – individuals seek to mitigate perceived risks by arguing that it may improve their commute, by saving time.

***MP1** – Thing is, if it makes your commute to work a lot better, then you’re gonna, ain’t ya?*

***MP5** – Yeah...*

(FG 10)

In the following argument, time is not as much the underlying mitigatory argument as is the commodity of new technologies. Despite the fact that the participant is not discussing it in the context of a smart city, it draws on their own experience in order to mitigate potential constructed risks. In fact, for them, smart home technologies are

a matter of comfort. For instance, turning on the heating before they come home so that they return to a comfortable temperature.

P7 - Um, I guess things like the central heating and, and the lights and things. We only have cats so it's not really a big thing. But it's nice when we're on holiday to put the heating on for a little bit and you can just or put it on just before you get home or something like that. Something we wouldn't necessarily [inaudible asides] be able to do, whereas they're our nest thing.

(FG 3)

In the last example of this code, the participant similarly discusses the use of smart home technologies – a smart doorbell - as an improvement to their daily lives. According to the participant, the ability to communicate with whoever is at the door (e.g., postman) from anywhere else (e.g. while on vacations) significantly improves their lives. Therefore, constructed risks from the use of these technologies may be mitigated by these benefits and the importance attributed to them by the individual.

There is, however, an issue warranting attention. The participant may also construct risk mitigation by arguing that this smart doorbell allowed them to surveil their dog sitter. Making sure the dog sitter came in and went out at the right time was clearly important to them. Thus, the intensification and mitigation of risk are dependent on the role of the subject (i.e., surveillor vs person surveilled).

P4 – If I bought that because I went on holiday for the whole six weeks and I was able to talk to my postman and tell him to, where to put my parcels [laughter].

P1 – I love that [overtalking].

P4 – And to make sure my dog sitter came in at the right time and go [laughter].

P1 – And make sure she was coming.

P4 – So for personal, um, use...

P1 – Yes.

(FG 6)

5.5.5 SOCIAL

Use of social-related mitigatory argument were coded 5 times. These arguments pertain to the individuals' social status and recognition desires to be met, and whether or not the data donation programme was socially accepted. In other words, individuals mitigated risks of giving their personal information if the programme was used by

several individuals, it had satisfactory reviews, or, if it, somehow, increased their social standing. All these domains are characteristic of a social dimension.

In the three examples below from focus groups one, three and four, mitigatory arguments referring to the importance of social proof as a way to mitigate possible perceived risks are displayed. The importance of the volume of participants, together with what these think and say about the data donation programme constitute an important factor in the decision to participate.

P7 – Yeah, pretty much. Depends how popular the app is though, to be honest. As you said, as you said, if you see loads of other people using it, you wouldn't really care as much, but then, if there was only a few people using it, you'd be a bit more sketchy, especially with the reviews on, like, Google Play for instance.

(FG 1)

P7 – And it'll be peer to peer recommendation about whether to use the app. I only use it because Matt uses it and he only uses it because he'll uh, his cycle buddies use it, yes [inaudible asides].

(FG 3)

P4 – Or you'd ask other people if they'd done, uh, signed up to it before or somethin' like that, before you actually sign up to somethin'.

(FG 4)

5.5.6 PERFORMANCE

The performance code was ascribed 60 times. Arguments pertaining to this code included the performance of the entity collecting their personal data and the participants' demand for reciprocity and feedback. Arguments such as holding the city council accountable for the conditions of the road and the expectation to receive something in return, even if it is as basic as feedback about their health, for their participation were ascribed this code. Similarly, arguments referring to the need for reciprocity or feedback from the app or city council were also assigned this code. That is, although the individuals could be willing to donate their personal data, they expect to receive, for instance, feedback about their health or fitness levels.

The exchanges below illustrate some of the arguments pertaining to 'performance' mitigatory code. For example, in the exchange below, participant four argues that they would still participate in the smart city project "because it's not going to fix [the potholes and road issues] if nobody tells". Thus, the ability to hold the city council accountable is a mitigatory argument pertaining to the 'performance' code.

P2 – I, I think still be more inclined to because it's [overtalking]...

P4 – Yes, because it's not going to fix if nobody tells, says that there's a problem.

P2 – Yes, because...

P4 – It has to be mentioned, doesn't it?

P2 – Yes, if there, if it is about making their travel to work or wherever they're going better.

P4 – If it's beneficial, yes.

(FG 3)

In the argument below, participant four, from the focus group six, goes to the extent of claiming that they would not participate “for no good reason”. Therefore, an incentive to participate in the form of, for example, repairing the potholes reported, would suffice for the individual to be willing to donate their data. In this example there is not only a demonstration of a demand for accountability but also a wish for reciprocity. In this case, reciprocity need not to be in financial terms – this will be discussed later on – but in the form of keeping the council accountable for, in this particular case, the conditions of the road.

P4 – So I would not be putting an app on my phone purely for no, for no good reason, so if there was maybe an incentive to, I suppose, if they could say the pothole might be repaired. That might be a big enough incentive...

P1 – Yes, yes.

(FG 6)

Lastly, pertaining to this code, the ability to receive insights about the data donated (e.g., feedback about their health and fitness levels) would be enough of a reason to mitigate risks and be willing to donate their personal data and participate in the smart city project.

P4 – Um, and you are getting something back. So, you're getting your heart rate, which we're all actually quite interested in doing in keeping fit and healthy hopefully, [inaudible asides]. But then the personal, personally it wouldn't bother me at all, not that would know.

(FG 6)

5.6 CONCLUSION

In this section the coding structure was presented together with the rationale behind the codes and some representative examples from the focus groups. Codes pertaining to the identification and reinforcement of risks were attributed based on privacy-specific, and traditional risks of donation, respectively. Thematic analysis of the focus group discussions relating to the reasons for donation revealed that themes relating to the traditional donation risk categories (i.e. Mitchell 1999 and Barkworth et al 2002) also worked to mitigate the constructed data donation concerns. As such this chapter concludes that the thematic basis for risk identification and the mitigation of constructed risks is similar. Furthermore, whilst all of the a priori risk categories are present in the discussion, the question remains about the extent to which the privacy risks and traditional donation risks interweave with each other to either reinforce or mitigate the constructed risks of donation. Such an analysis is presented in the next chapter.

Chapter 6: MAKING SENSE OF THE CONSTRUCTION OF RISK

6.1 INTRODUCTION

This chapter interprets the codes identified in the previous chapter, and analyses how these are integrated in the participants' arguments and interactions as they construct the risks associated with data donation. This chapter is divided in two sections: identification and reinforcement and mitigation of constructed risk. However, when referring to 'mitigation' of risks, the author is referring to the arguments exchanged that would diminish the impact of the constructed risks or make donating data an acceptable practice in the eyes of the participant. This thesis does not reflect a positivistic notion of risk, therefore, when referring to risk henceforth, the author is referring to the mitigation of the constructed risk by the participants. The objective by laying out the chapter discussing the identification and reinforcement and mitigation of construction risks is not to position the positives against negatives of data donation. Instead, this chapter aims to find the fluidity in how individuals construct risks through the arguments made in the focus groups. Although one can observe a trade-off narrative in participants' arguments, the focus of this research is on understanding the interplay between arguments and how these support the construction of risk by the participants. Specifically, it is considered how the types of risk highlighted by the different frameworks interplay with each other in the coded text to form overarching

themes. Moreover, it offers examples from the focus groups data to support the patterns and themes identified.

The first section examines the interplay between risk categorisations within the arguments where risk is reinforced. Initially, when participants constructed different risks of engaging with the city council's smart city programme, they did so by identifying privacy specific risks. These risks were then reinforced by the same individual, or by their peers, by rooting their arguments within the traditional donation risk framework. Therefore, although the risk construction was initially based on a privacy-specific dimension, the participants reinforce the risks by discussing possible unwanted consequences rooted in the traditional donation risk dimensions (Barkworth et al., 2002).

In the second section, the risk mitigation patterns are presented and discussed. In this case, participants once again used arguments that are found in the traditional donation risk framework (Barkworth et al., 2002) to mitigate privacy-specific risks. For example, an individual may mitigate the risk of data collection by claiming that by participating in the programme they can keep the city council accountable (i.e., a performance argument mitigating a data collection risk). Lastly, at the end of the chapter, an illustration of the dynamics of the discussed interplay is provided as a visual summary of this chapter.

6.2 MAKING SENSE OF THE CONSTRUCTION OF RISK

In this section the different arguments pertaining to how the risk was identified and reinforced by the participants are discussed. It aims to present, interpret, and discuss the patterns emerging from the focus group data and demonstrate how these are used to construct the different risks perceived in donating personal data. This analysis is based on the coding structure used to categorise the different arguments identifying and intensifying different risks during the focus groups discussions.

6.2.1 TRADITIONAL RISKS → PRIVACY RISKS

After analysing the coding structure and the underlying arguments, traditional donation risks work to intensify the privacy risks. Initially, throughout the focus groups, when a data donation risk is identified, it is expressed in terms of privacy specific risks. Following the initial risk identification, the following discussion and intensification process is accomplished using arguments pertaining to the traditional donation risk framework. In other words, privacy risks do not tend to be spoken about in their own terms but discussed in relation to a traditional risk. Accordingly, the traditional risk framework tends to assert the negative consequences of the expressed privacy risks. When presented with scenarios depicting either a neutral data donation situation, as is the case of the first scenario (see section 7.4.2, and appendix 3), either a situation where there may be a risk or consequence portrayed, as is the case of the last scenario, the participants followed that same response pattern. Accordingly, in a

first instance, after the scenario is presented and some basic remarks made, privacy-related risks were identified (e.g., concerns regarding the way the data collected or what kind of data is being collected). As an example, in the following cases, the participants' first clear concern is with what is going to happen with the data. In other words, who is collecting the data, what kind of data is being collected, how long is it being held for, among other things. All issues relate to data collection.

P1 – How do you check where your data is gonna go?

(FG 2)

P4 – What are the Ts and Cs?

P5 – Yes [overtalking], absolutely, how the data is secured?

P3 – How long it's held for?

P1 – Yes.

(FG 5)

These risk identifications are not always clearly expressed by the participants. Often, the identification of the risks is implicit, but discernible when the individuals voice

and discuss their concerns. In the following cases, the participants use traditional risks to intensify a privacy risk that was not previously clearly expressed, but that it is evidently implicit. For example, although not claimed, when the individual is worried that someone can stalk them, they are perceiving a consequence of an identified data dissemination risk.

P1 – [...] yes, someone could stalk me on Strava.

(FG 2)

P3 – And, if he's in a particularly secluded area, say the Redways around here, some of the parts you could be in could just be bushes and it can be a bit frightening sometimes if you're there on your own. So, if you were always at that point at a certain time, early morning or later on in the evening [overtalking].

P2 – Be in trouble.

P1 – It's a safety thing.

(FG 7)

Nevertheless, not every traditional risk intensifies a privacy one. Instead, some specific traditional risks appear to intensify specific privacy risks. The table below illustrates the pattern that became apparent in the focus groups data. These specific interplay dynamics will be discussed over the next sections.

Risk Identified	Intensification
Data Collection	Psychological Time Performance
Data Processing	Financial Psychological Performance
Data Dissemination	Psychological Physical Financial Social Performance
Invasion	Psychological Performance

Table 7 - Risk Intensification Dynamic

6.2.2 INTENSIFICATION OF DATA COLLECTION RISKS

This section shows how data collection risks are intensified by concerns about the performance risks of the organization collecting the data, psychological risks and time

risks. Concerns relating to the potential risks of data collection were the most prevalent in the participants' arguments with 122 instances coded. After identifying a data collection risk in a given scenario (e.g., how the data is collected, what kind of data is collected, etc.), the participants intensified these by arguing whether the organisation collecting such information is worthy of their trust, what kind of data they are receiving (e.g., how personal is it), and what will that data inform about them. These arguments clearly depict concerns regarding the performance of the entity collecting and, ultimately, holding their personal data. In the example below, the participant is talking about the risks of data collection arguing that they do not "see bad things" in giving such personal data to the city council. However, by focusing on the performance of the entity collecting the data, in special, how secure their personal data is in their hands, the participants are identifying a risk in tandem with a data collection risk. Performance, in this case, does not intensify a perceived risk but represents another dimension of the identified of data collection.

P5 – I wouldn't say I see bad things, but I'd say at least Kris needs to have confidence in the people collecting the data, that they are secure with, with what they're doing, they know what they're doing.

(FG 1)

Individuals are not solely concerned with the performance of the entity that collects their data. There is also a psychological implication to the collection of personal data. Returning to the example already cited on section 5.3.1, the participant number four

of the focus group ten was anxious about the amount and kind of data being collected (e.g., how personal that data was: “nose size”). The participant hyperbolised the scenario by using extreme examples of the types of data being collected. There is a clearly defined identification of the risk perceived in the scenario. Then, the intensification that followed was based on a psychological argument: “a bit too personal”. By claiming that the data being collected is beyond what they were initially comfortable with, and, it has now reached a “too personal” level, demonstrates uneasiness with the data collection process. This psychological uneasiness is depicted by the hyperbole used in the participant’s argument. In fact, when building their argument, the overstatement of data points collected featured only physical characteristics. The participant culminates their argument by claiming “Like yeah okay I’m fat (...) don’t have to tell you about it every day” professing a psychological implication of the data collection.

***FP4** – No, what more do they want? Oh my god. They’re gonna want foot size, nose size, hand size, what else size [overtalking]. There’s gotta be a point where you’re gonna have to stop. Like yeah okay I’m fat, that’s, you know, don’t have to tell you about it every day. That’s... I think that’s just plain...*

***MP1** – A bit too personal I think.*

***FP4** – I think that is a little bit too personal, yeah.*

(FG 10)

Additionally, in the example below previously presented in section 5.3.1, the participants were initially worried about when and for how long was the application collecting their data. However, this perceived data collection risk was immediately intensified by a concern of whether the council will have knowledge of their excessive speeding behaviour while driving. Therefore, the initial identification of a privacy specific risk was intensified by a psychological risk: the participant was worried about the potential consequences deriving from the city council's knowledge of their driving behaviour.

P4 – What about driving as well? If you're driving a car and you speed, it's got all your speeding [laughs], it's got your speeding as well.

P1 – Yes, I was going to say is it recording [overtalking] all, all the time, then?

P6 – Oh, oh that's not good [laughter].

P1 – Is it all, all the time? So, it's not whether you're cycling or not, it's just all the time?

(FG 5)

Lastly, the impact data donation has in an individual's daily lives is another consequence intensifying the constructed data collection risks. If the process of

donating personal data is cumbersome or takes longer than the individual expects, then it is constructed as a risk by the participant. For example, in the exchange below, also depicted in the section 5.3.8, the participant asks whether reporting issues with the road could be done when Kris got to work, or at a later time. In this case, the individual is trying to understand if the donation is going to take time, and how long will it take. Confused with the scenario, the participant asked the moderator if stopping to take a picture and report the issue is absolutely necessary, to which the moderator questioned whether that would impact their decision to participate in the city council's programme. The participant indicated that yes, indeed stopping all the time they find something to report would become a nuisance and a waste of time.

P6 – If you travel every day that way, surely he could report it when he got to work or at another time, or not? Would you have to do it there and then?

I – Would that impact your decision?

P6 – Well, yeah, because if he's finding things on the way all the time, I mean, you're not gonna keep stopping.

(FG 10)

Similarly, in the argument below, not yet presented, the participant clearly details that if donating that data would mean leaving ten minutes earlier to work, anticipating the presence of issues to report along the way, some sort of incentive would be expected.

This argument illustrates a concept that if donating data takes longer than one is willing to give, it becomes a job. As a consequence, jobs come associated with an expectancy for rewards.

One could argue that time risks are also associated with other types of donation, as for example, blood donation. However, people still donate without expecting any payment. Nonetheless, as explored during the literature review chapter, individuals donating blood still receive something in return. Depending on the country, it may not be of monetary value, or even tangible (e.g., a fast-track at hospital emergency rooms), it may just be the experience of a ‘warm glow of giving’. In the case of donating data to a smart city, it is harder for the participants to conceive the positive impact their contribution may have for the city and its citizens.

P7 – There’s no initiative for, there’s no incentive for, or not that we’ve heard, for Kris to do it. So, if she has got to leave say, I don’t know, ten minutes earlier knowing that she’s going to have to stop a couple of times or potentially have to stop a couple of times. And then [unclear] if she gets to work earlier because she didn’t have to stop, she’s not being paid for that extra time so it’s a bit of a... She’s actually giving a lot more than I think, including the information, plus her time which is the opportunity cost of that time. Uh, the council aren’t really giving her anything in exchange...

(FG 3)

6.2.3 INTENSIFICATION OF RISKS RELATED TO DATA PROCESSING

In relation to data processing risks, participants demonstrate a concern about the way their personal data is handled by the entity collecting it - for example, if their data is being used for the purposes to which they initially consented. Furthermore, the perceived risks associated with data processing may also refer to the discomfort an individual may express by the way their personal data portrays them to the organisation processing the individual's information – for example, whether different data points can indicate their political preference without the individual disclosing it. The intensification of these data processing risks is argued by recurring to the use of arguments associated with financial and psychological risks. The performance dimension is also present, although in tandem with the identified privacy risk. These arguments were, as with the intensification of data collection risks, discussed as concerns for the potential consequences stemming from the way the institution handles the individual's personal data.

For example, in the case below, the participant is afraid that, by donating their personal data, they may be excluded from an NHS service. If, for instance, their daily steps and the general level of physical activity would become key decision variables of what service one could have access to. In this instance, the identified data processing risk is implicit and intensified by psychological, and [potentially] financial consequences. The consequence is psychological in the way that the participant is fearful of the potential consequences of data donation. Equally, the individual also expressed a

concern of being excluded from an NHS service, which, ultimately, can have financial implications should they have to procure treatment privately.

The construction of performance risk is also present as the participant does not fully trust that the data is going to be used for what they consented to and is worried about a potential secondary use. However, as previously claimed, this performance risk is related to the identification of risk, at par with data processing, and it is not described as a potential consequence.

PA5 – It would make me very suspicious. If you think about when we look at the NHS [overtalking] and what they're talking about. How they're talking about sort of reducing certain services for certain people. Whether they're going to be obese or if they're smokers, you're not going to be able to get certain sort of medications for different conditions. I know, I can't help but think that could this data, maybe not now...

PA6 – Yes, but in the future.

PA5 – Be applied to that sort of thing.

(FG 7)

In the example below, the participant claims that the gathering of information does not really bother them. Instead, the constructed risk related to how that information is

going to be used. This was the way that the participant initially identified the privacy-specific risk of the scenario being discussed. However, the individual continued their argument by wondering if their personal data was going to be used to nudge them to be more active. This constructed psychological risk of being judged based on their physical attributes led the individual to be more cautious of using the app.

PA2 – Information. It like doesn't... It wouldn't really bother me, but it just... It's... I mean, it... What...? What are they going to use it for? Is it for them to then turn around at the end of it and say, well, should cycle more because [overtalking].

(FG 8)

This example of the focus group interaction follows the same pattern as previous cases: the participant identifies a risk by basing their argument on one of the privacy-specific risks. Subsequently, the same participant, or others throughout the discussion, intensify the initial risk constructed in the group discussion by rooting their argument in one of the traditional risks. This intensification happens by associating these as possible unwanted consequences of the identified risk.

6.2.4 INTENSIFICATION OF DATA DISSEMINATION RISKS

In respect to the constructed risks concerning the data dissemination category of the privacy-specific taxonomy, participants were very responsive with instances referring to this category being coded 90 times. In fact, from the four categories of potential data misuse introduced by Solove, the risks associated with data dissemination were the most perceived and discussed. Consequently, when this risk was identified, its intensification was built on four out of six possible traditional risk dimensions: physical, psychological, social, and financial. As with the previous section, the construction of performance risks was also present, although at par with the data dissemination initial concern.

Furthermore, it is important to note that the pattern of risk construction in this case continues to follow the same method as the previously discussed categories: when intensifying the previously identified privacy-specific risk, the use of one, or more, traditional risks is presented in order to illustrate possible consequences. For example, in the quotation below, the participant clearly intensifies the risk of data disclosure (i.e., a third party knowing the route an individual takes), by claiming a potential physical risk as a consequence.

P3 – If I, if someone else had that information I'd be seriously worried.

P1 – Oh my gosh, yes same.

P4 – Yes that would be very concerning.

(FG 6)

In fact, after someone identified this risk, another participant immediately used another traditional risk to continue the intensification process.

P1 – As soon as you started talking about it, I thought, yes, someone could stalk me on Strava.

(FG 2)

In this case, however, as stalking is not only a potentially physical risk, but also a psychological one (Logan and Walker, 2019), both constructed traditional dangers are used to intensify the initial privacy risk of data dissemination.

P3 – I've never thought about when I first started cycling, I got, um, someone recommended an app called Strava. So, I uploaded that and then it wasn't for about a month until somebody I'd started to cycle with regularly messaged me privately and said, you do realise your, all of your start and finish things are at your garage. So, people know where your bike is. So, if, like you say about getting connected, if you like the wrong person, by accident or on purpose. If

they think well hang on, I know Craig's got a bike, that's where all his journeys start and stop, they then know where you keep your bike, amongst other things.

(FG 5)

In the example above, the participant did not speak about the risk of their personal data, such as location and routes taken, being accessible by others until their friend told them. Nonetheless, when the participant was advised that sensitive data was being shown to everyone (i.e., data was being disseminated), the intensification of the risk was done by resorting to one of the traditional risks. In this case, the risk of getting their bicycle stolen (i.e., financial risk).

Furthermore, when the participant says “*amongst other things*” it is indicating a perception of other risks beyond getting their bike stolen. For example, being kidnapped or stalked.

P3 – And who is looking at it? Is it just the people who want to know about the potholes or is it the wider community? Because people will get to know where Kris is at what time? And, if he's in a particularly secluded area, say the Redways around here, some of the parts you could be in could just be bushes and it can be a bit frightening sometimes if you're there on your own. So, if you were always at that point at a certain time, early morning or later on in the evening [overtalking].

P2 – Be in trouble.

P1 – It's a safety thing.

P3 – People would know that [overtalking].

P1 – Put yourself at risk, really.

P5 – Or, even if Kris was alone and he's out on his commute, a Billy burglar is quite happy at home nicking his Xbox [overtalking].

(FG 7)

P3 – I used to be a member of a cycling group just up the road. And, they had tracked on Strava or one of these other apps what type of bike they had, how old it was, when they changed their tires to new ones. When they did this, this and this. And, he had an expensive bike. And somebody followed him on Strava and pin-pointed his address and stole the bike from the garage.

P2 – You see?

(FG 7)

In the above example, the participant draws on their own experience to demonstrate the possible consequences of others knowing their location. In other words, the financial burden of having their bicycle stolen, and the psychological impact of being the victim of a crime. In the case of data dissemination, the intensification is done by thinking about or attempting to hypothesise about the consequences of such risk: ‘If they disseminate my data, my bike can be stolen, I can be stalked, killed, or mugged’. Social risk is also present as a perceived consequence of a data dissemination risk. For example, in the interaction below, the participant claims that they would like their son to use the technology so they could track him. This argument potentially indicates an intention to use technologies as a mitigation for given risks (e.g. physical risk). Nonetheless, this mitigation interplay is later discussed in this chapter. The focus here is on what the participant argues next: *“But, you know, I don’t want my husband looking me up and seeing where I am”*. Here the same use of technologies shifts from being a mitigatory argument, in the case of their son, to an intensifying, if it applied to the participant. Should the participant’s husband be aware of some of their behaviours that, perhaps, are not socially approved, or not approved by their husband (e.g. shopping or eating out too often) this may have an impact on their social.

Furthermore, another interesting observation is that in this exchange of intensifying arguments, another participant intensified the perception of the data dissemination risk by claiming that their partner judges them on their consumption habits (e.g. “are you in Costa again?”). In this particular case, it is the fact that the individual is often at Costa Coffee that raises the judgement from their partner. Consequently, the participant who initially identified the data dissemination risk, responds to the

individual by giving an example that depicts social judgement on their shopping habits. In this example, previously discussed in section 5.3.9, not only a psychological risk that feeling judged represents is present, but also the constructed risk of what their social group may think of them should they become aware of certain habits or behaviours.

P6 – I want to have it on my son's when he goes. But, you know, I don't want my husband looking me up and seeing where I am.

P1 – Oh, it's terrible. He used to be like why are you in Costa again? [Laughing].

P6 – Yes, people are like, why are you out clothes shopping? No, I'm not. You are in Next. What? [Unclear] I'm fine. [Laughs].

(FG 7)

In addition to all the risks discussed and exemplified above (physical, psychological, financial, and social), it is now important to turn the attention towards the performance risk, another category of risk belonging to the traditional risk framework. The performance risk, unlike the previous risks from the same framework, was not discussed as part of a mitigatory argument. Instead, this dimension is often a perceived risk at par with the privacy-specific risks. When individuals blame the city council for their data having been misused, as is the case of data dissemination, there is also an

element of erroneous performance from the city council in handling people's data. For instance, in the exchange below, although the risk identified is of data dissemination, participants are still referring to performance as an explicit risk on the same level of data dissemination. This exchange illustrates that although there was a financial implication from the data dissemination, the participants' frustration stems from the fact that the council betrayed their trust. In other words, there was a performance issue, in this case the fact that data was disseminated without prior consent, that lead to financial consequences.

P3 – Because you had your trust with the council when you got the smart, you know, smart watch and all that stuff, you, you know you trust in the council, with your data...

P1 – With your information.

P3 – And depending on what was on the fine print, you just went ahead with it. Didn't think it would go over to a car insurance...

P1 – Your car insurance, why would you be, why would you go to your car insurance?

(FG 6)

6.2.5 INTENSIFICATION OF INVASION RISKS

The invasion risks relate to the individuals' concern that, by donating their personal data, they will be targeted by nuisance calls or spam e-mails. This risk is, as with the other privacy specific dimensions, intensified by risks akin to the traditional framework. Specifically, invasion risks are intensified by the possible negative psychological consequences, which are, for instance, feeling judged for receiving a certain targeted ad, and feeling like a line has been crossed. Additionally, similar to the former sections, performance risks appear in tandem with the privacy-specific risk. That is, individuals perceive not only the risk of being invaded by, for example, nuisance calls, but also that it would be the city council's responsibility for the fact that they were being disturbed.

In the interaction below, previously presented in section 5.3.4, adds another layer of analysis in that besides being an identification of an 'invasion' risk, the participant intensifies it by arguing a psychological consequence of that invasion. Specifically, the participant identifies an invasion risk (i.e., the fact that a "Slim Fast" advert is constantly appearing), however, and despite the fact that the individual realises they "have been spied upon", the intensification of the risk is done by illustrating a psychological consequence: "they are giving me advertisements for my weight. Problem which I wasn't aware was a problem". Furthermore, this participant claimed that prior to being targeted by these nuisance advertisements, Kris, "was happier with herself".

In fact, it is not so much the fact that they received a targeted advertisement, but the reason behind why they received this targeted advertisement that concerned them. Whether it was because, after donating personal data, someone understood that Kris was overweight, or not as active as they should be. Whether it was because Kris was commenting about struggles with weight with their friends. Or was it, perhaps, because Kris had searched “how to lose weight” online. Possibly due not only to the fact that the participant received the “Slim Fast” advert, but because, somehow, someone (or some system) believes that they should lose weight. These uncertainties, and lack of technical knowledge typical to the general public feeds into the psychological unease experienced by privacy invasion risks.

FP4 – There’s SlimFast keeps popping up [laughter] and you’re like, right, okay, yeah, I’ve been spied upon here.

MP2 – You’re thinking, well why has he got that? He must be [overtalking].

FP4 – Especially as a woman. They could be... Kris is, you know, a woman again. And she’s like, oh my goodness, they’re giving me advertisements for my weight. Problem which I wasn’t aware was a problem. And she was happier with herself.

(FG 10)

As with the previous privacy-specific dimensions, performance risks are also present in this dimension in tandem with the initially identified risk, and not as an intensifying argument. In the example below, the participant claims that just because they signed up for something online, they start being “inundated” with unwanted e-mails from third party companies. The individual believes that, by signing up for something online, they sold their e-mail address to a “massive list” of companies.

P3 – I sign up for like stuff online or whatever and then, you know, a couple of days later you just get inundated with other companies sending you emails about what, you know, this and that. And, it's like you're getting all this. You just sold your email address on some massive list to people. Do you know what I mean?

(FG 8)

6.3 MAKING SENSE OF THE MITIGATION OF CONSTRUCTED RISK

In this section the different arguments pertaining to how the risk was mitigated by the participants is discussed. It aims to interpret the emerging patterns from the analysis of the focus group data and demonstrate how these are used to construct the different risks. This analysis is based on how the codes identified in the transcripts were used

to mitigate the previous identified and intensified risks involved in donating personal data.

Risk Identified	Mitigation
Data Collection	Saving Time Performance Financial Benefits Physical Safety Psychological Social
Data Processing	Saving Time Performance Financial Benefits Physical Safety Psychological Social
Data Dissemination	Saving Time Financial Benefits
Invasion	Financial Benefits

Table 8 – The Dynamic of the Mitigation of Constructed Risks

6.3.1 TRADITIONAL MITIGATORY ARGUMENTS → PRIVACY RISKS

Individuals seek to mitigate the constructed risks, as expressed in order to avoid the potential consequences as outlined in sections 6.2.1 and expressed in table 7, or to improve their lives (e.g., save time commuting). In order to mitigate these constructed risks, participants make use of arguments pertaining to the traditional framework. For instance, a participant wants to use an app because it will allow them to know where their children are at all times, thus feeling safer and assured that their children are

secure. This argument may mitigate any constructed privacy-specific risk related to the individual's participation in the smart city project.

As demonstrated throughout section 6.2, summarised in table 7, traditional risks are constructed as consequences of privacy-specific risks – individuals look to mitigate the initially constructed risk rather than the consequence. If the constructed privacy risk is mitigated by the potential benefits the technology may offer, then it is worth to participate in the smart city project and donate their personal data. Therefore, the consequence constructed by the participants is not directly mitigated, instead, what is mitigated is the initially constructed data dissemination risk. For example, “I want my Strava data to be disseminated to my family, so they know where I am at all times. This way I will feel safer”. This quote demonstrates that the constructed dissemination risk can be mitigated if the information flows to the participant's family, and from that, they will feel safer and protected. Interestingly, Nissenbaum's theory of contextual integrity accounts for this ‘appropriate flow of information’.

6.3.2 MITIGATION OF THE CONSTRUCTED DATA COLLECTION RISKS

When compared to other privacy risks, the constructed risks pertaining to data collection were mitigated by the largest number and type of arguments. Participants argued that they would participate in the city council's smart city programme if that meant their lives would be improved (e.g., saving time commuting). Other reasons to participate in the programme included the opportunity to keep the city council accountable, whether they would receive financial benefits, protection against physical

or psychological dangers, or if their friends, or a large number of people, recommended it. For example, in the discussion below, the participant argues that using Strava, a sports tracking app, and let their [location] data being collected improves their (feeling of) safety. Should something happen, the individual's family knows their whereabouts.

MP1 – So, with Strava, you can, you can err, log on, you can log on with your family so they can see where you're actually going live. So, if anything happens to you...

FP4 – Oh yeah that's an app I was thinking of. Yeah.

(FG 10)

In the following argument, the participant mitigates the constructed risk of data collection (i.e., being constantly tracked), by claiming that the city council would act quicker in maintaining the city's infrastructures. Specifically, if donating their data leads to an improvement in their city's conditions, the individuals would be more willing to participate in the smart city programme. This is due to the fact that donating data would mean an improvement in their daily lives (e.g., potholes get fixed quicker). Although this aspect would benefit all citizens, participants' arguments reflect a certain selfish thinking (i.e., their own personal benefits and the way their own lives would improve from this).

MP5 – Which is going on, yeah, with all the, all the tracking. But then, then there's another side to it where the authorities are looking at erm... What do they call it? Err, smart maintenance. Right, so they're looking at your street and they're looking at your entire street. Not to catch people walking down but to see, is there a pothole there? Get somebody out to do that automatically. Is that light out? You know, all that sort of stuff.

(FG 10)

Next, the participants discuss whether Kris gets to keep the Fitbit should s/he decide to participate in the city council's programme. At the end of this short exchange, one participant claimed that "there's gotta be some perks in it, otherwise it's not... No point in doing it at all, is there?". Here, the individual clearly seeks some sort of financial benefit in order to incentivise their participation. If no benefit was provided by the city council, then engaging in the programme by donating their data would not be enticing enough. There would be no [financial] mitigation of the possible consequences stemming from allowing the local government to collect their personal data.

P6 – Um, and does he get to keep the Fitbit?

P1 – Yeah that's a good question, do I get to keep the gadget? What's the perk?

[Overtalking]

P2 – [Overtalking] free Fitbit.

P6 – The gadgets. If they're gonna give more for his bike as well.

P3 – Yeah. There's gotta be some perks in it, otherwise it's not... No point in doin' it at all, is there?

(FG 4)

The next two interactions further the above argument in that financial benefits are a key data collection risk mitigating factor: “I think incentive is a big part of it”, “I don’t give in my details to anything unless I want to be buying something at a discount...” or “ ... if you don’t find out what the information’s going to be gathered for and you don’t feel a benefit, I don’t think that it’s something people would be interested in doing”. These are some of the strongest claims made by participants in order to mitigate data collection risks. One can see an exchange logic running throughout the participants’ arguments. Privacy here appears as economic thinking (benefits vs risks): “Does Kris get an incentive like a free bike or something?” participant six, from focus group six wonders as if the fact that receiving an incentive may suddenly outweigh the potentially constructed risks.

P6 – Does Kris get an incentive like a free bike or something?

P1 – Yes, cheaper discount on the bike through works, through her work scheme.

P6 – Yes, something.

P4 – Yes, I think incentive is a big part of it.

P1 – Yes.

P4 – Because I don't give in my details to anything unless I want to be buying something at a discount...

P1 – That's going to benefit us.

(FG 6)

P4 – Um, but if you don't find out what the information's going to be gathered for and you don't feel a benefit, I don't think that it's something people would be interested in doing.

P5 – No.

(FG 6)

P6 – You can do it, like, to incentives as well. So, you, you can link your fitness watch to, um, like life insurance like Vitality life insurance...

P1 – Yes, so you get all the discounts.

P2 – Yes, mm-hmm...

P6 – And if you do so many steps a day you can get cinema tickets...

P1 – Costa coffee or Starbucks...

P6 – And you get discounts on things. And all sorts.

(FG 6)

Next, a participant argues that the potential risks of data collection can be mitigated if the app is popular. The number of people using an app or participating in a data donation project, as well as what they say about it (i.e., their reviews) is a mitigating factor of perceived data collection risks. Therefore, these quantitative (e.g., number of people using the app), and qualitative aspects (e.g., feedback given by the users) influences an individual's decision on whether to take part on data donation programmes.

P7 – Depends how popular the app is though, to be honest. As you said, as you said, if you see loads of other people using it, you wouldn't really care as much, but then, if there was only a few people using it, you'd be a bit more sketchy, especially with the reviews on, like, Google Play for instance.

(FG 1)

Lastly, an interesting surveillance mitigatory position is the 'nothing to hide' argument. This argument refers to the individual's passiveness and lack of concern for data collection due to the fact that, as they claim, they have nothing to hide from the entity receiving their personal data. Therefore, they disregard potential risks of data collection in the conviction that the possibility of potential consequences for them are practically null. Nonetheless, according to these individuals' argumentation, those who have something to hide (e.g., criminals) are the ones who will oppose to having their personal data collected.

The 'nothing to hide' argument illustrates a mitigation of privacy risks by attempting to rationalise and dismiss the risk of donating data. This psychological mitigation of the data collection risk sees the individual ease their concerns by distancing themselves from the possible consequences of giving their personal data. For example, in the argument below, the participant claims that, as they are "law-abiding citizens" they have nothing to worry. And, they have nothing to worry, because their data is only being stored and not "monitored" (i.e. processed). Therefore, the individual does not have to fear potential consequences of data collection.

P7 – People that are law-abiding citizens don't need to worry about that. Because their, it's their data that isn't being, being monitored as such. Well it is, it's being stored. But it's not being looked under...

P4 – For any harsh reason or anything, yes.

(FG 3)

When speaking about mitigation of data collection risks, participants were often very candid: If donating their personal data may result in an improvement of their lives (e.g., financial benefits or shorter commute), or, if it may result in a potential reduction of the chances of other risks occurring (e.g., feeling safer if something happens) individuals would happily do it. Equally, if the volume of users, together with their opinions, is satisfactory enough for the individual, they would also participate in the programme. However, it is important to note that it is not possible at this point, nor is it the focus of this research, to understand the weight of these mitigatory arguments in an individual's decision to donate their data.

6.3.3 MITIGATION OF THE CONSTRUCTED DATA PROCESSING RISKS

When compared to the mitigation of data collection risks, the dynamic of the mitigation of data processing risks is identical. Participants mitigate risks pertaining

to data processing in order to keep the city council accountable, if that meant receiving financial benefits, protection against physical or psychological dangers, if their friends, or a large number of people, recommended it, or if that meant that their lives would be improved (e.g., saving time commuting).

For instance, in the quotation below, participant four from focus group four argues that processing their personal data (e.g., photo taken to pothole and submitted through the app together with geolocation data), in order to hold the city council accountable (e.g., fixing potholes), would be a reason to participate in the smart city programme by donating their personal data. In this example, a performance argument mitigating a data processing risk can be observed.

P4 - If you, if you were takin' a photo of somethin' that said, look, beware. This is... And it's goin' out to a wider people, that's... I think that's more than incentive in regards to getting fixed, stuff fixed, and all that sort of stuff.

P1 - Yeah.

(FG 4)

The exchange below between participants three and six from focus group seven, depicts financial, as well as physical safety, benefits mitigating data processing risks. Participant three claims that with a 'black box' installed in one's car, and thus letting the insurance company process their personal data, would not only reduce their

insurance premiums (i.e., financial benefits), but would also affect their driving behaviour (i.e., physical safety).

P3 - With like the black box and young drivers that we were talking about. Um, it's proven, isn't it, that actually, that has a bigger impact? It's not just it brings down the premiums, but actually affects the way that they drive.

P6 - It helps the, yes. No, definitely.

P3 - And then, it stops sort of accidents and the rest of it.

(FG 7)

6.3.4 MITIGATION OF THE CONSTRUCTED DATA DISSEMINATION RISKS

In relation to the mitigation of data dissemination risks, the focus group discussions seem to concentrate on avoidance of consequences rather than on improving their lives. Focus groups participants, as part of the discussion, mitigate data collection risks in a myriad of ways (e.g., improve their commute), as discussed above. However, when discussing issues relating to data dissemination, where participants can easily picture possible consequences (e.g., insurance price hike), mitigatory arguments appear as trying to diminish the chances of certain risks materialising, or if it would bring them some benefits. For example, during the exchange below, a participant

claimed that it is the consequence of the data dissemination that bothers them. If, instead of an increase in their insurance premium, the dissemination of their personal data led to a discount, the individual would be pleased.

P6 – But I think it's the consequences that's really been the issue then, because if it'd been the other and they'd and they'd, um, the council and given the information to the car insurance company. And the car insurance company had said, oh we, we realise now that you're commuting to work by bike five days a week, therefore we're going to drop your premium...

P1 – That's... drop your premium, yes, yes [inaudible asides].

P6 – [Overtalking] Probably going to be pleased...

P1 – Exactly.

P6 – So actually I don't think its so much the disclosure of the data [overtalking]...

P3 – It's what happened.

P1 – It's what happened, yes.

(FG 6)

In the example below, a similar line of argumentation is being offered by a participant. For this individual, if he noticed an increase in premium, they would be upset. However, if they have gotten something in return for donating their data (e.g., city council paid them for participating), they would feel that everyone got something in return. Although they were hit by the consequences of their, perhaps erratic, driving behaviour, and by the city council's data disclosure, they feel that, if they got paid for it, it would be somewhat acceptable. Nonetheless, the participant still claims that they "will be mad at the end of it".

P2 – I think it all goes to what you were saying. That if you do it and they reimburse you, even if in... Yes, they came back and said, oh, your insurance has gone up blah-blah-blah. I was being ... reimbursed for that six months, so, yes, I'll be sort of inched off. But, again, be sort of like, okay, fine they've reimbursed me, they've paid me for this study for six months and whatever, so it must be something that... Look, they're getting something, I'm getting something. Yes, I'll be mad at the end of it if I find out my insurance is high, but I did get something for participating.

(FG 7)

6.3.5 MITIGATION OF THE CONSTRUCTED INVASION RISKS

The mitigation of invasion risks was expressed as an opportunity to improve the participants' lives through promotional messages with discounts, they may find useful in their daily activities. For instance, in the exchange below, participant two argues that companies that collect their personal data gets to 'know them better than they know themselves', followed by participant three arguing that they used to receive many "irrelevant" promotional communications, however, as these companies now have their personal data, they tailor the offers to their profile, thus deriving a constructed benefit from this interaction. The invasion risk is, here mitigated by a potential financial consequence that may improve someone's life.

P2 - They know us better than we know ourselves [laughing].

P3 - Oh no, it's better for me... I, I used to think that 'cause I used to get so many vouchers that were just irrelevant.

P2 - Hmm.

P3 - And now they only give me vouchers for things I buy.

P2 - Yeah.

P4 - Tailored to what you... Yeah.

(FG 2)

6.3.6 TRADITIONAL MITIGATORY ARGUMENTS → TRADITIONAL RISKS

Arguments pertaining to the traditional risk framework are used in order to mitigate risks of the same framework. This mitigation process, however, unlike the intensification interplay discussed above, is not interlinked. Different arguments were used to mitigate different risks. Rather than interlinked, they appear dependent on the benefits the mitigation would bring. In specific, the arguments used to mitigate the discussed risks relate to the creation of mechanisms to either avoid those same risks or to improve the individual's life. Therefore, arguments used by participants to mitigate traditional risks did not follow a clear pattern as was the case of the intensification arguments presented in the above sections. For example, in the quote below, the participant argues that they would not mind losing time reporting issues on the road on the way to work, because on the way back, if fixed, the journey would be easier and safer (e.g., the glass on the pavement would be cleaned up). In this argument, the individual mitigates a time risk with both time (i.e., saving time in their next commutes) and physical safety arguments.

P4 – Because you know, it might only take a minute or so, but you know it's going to be a lot easier 'cause you're gonna be going back that way anyway, aren't you? So if there is glass or anything you want that to be cleaned up, so if it takes an extra minute, you're late anyway aren't you, so...

(FG 10)

In the following example, the participant argues that if donating personal data would make their commute better, then they will participate. The individual follows up by claiming that if the roads remain with potholes, it will eventually damage their bicycles. Therefore, taking time to report these road issues is a small price to pay for avoiding expensive bicycle repairs. In this case, a time risk is being mitigated by arguing for the preservation of their assets (i.e., avoid future financial loss).

P1 – Thing is, if it makes your commute to work a lot better, then you're gonna, ain't ya?

P5 – Yeah...

P1 – Because, as a cyclist, if you hit a pothole on a road bike, you're coming off, and you're damaging your bike. If you hit it on a mountain bike, it's not a massive issue. Just roll with it. But I'd want a nice smooth [murmured agreement] if I'm on my road bike.

P5 – Yeah, repairing inner tubes cos of glass and all that. I agree with you totally.

(FG 10)

6.4 CONCLUSION AND FINDINGS

After examining the interplay of privacy and donation related themes in the focus group discussion, the key finding of this thesis has been established. It is concluded that although all participants initially identify the privacy risks of data donation, without exception these constructed risks are either intensified or mitigated by themes from one of more dimensions of the traditional donation risk framework. Traditional donation risk themes relate to the consequences of data donation and the consequences of engaging with a particular kind of privacy risk.

Not all traditional risk categories intensify the identified privacy risk. Specifically, data collection risks (e.g., having the city council collect one's data) are intensified by psychological, time and performance risks. Constructed data processing risks (e.g., the way the city council processes an individual's data) are intensified by financial, psychological and performance risks. Data dissemination risks (e.g., if the city council discloses an individual's personal data to a third party without their consent) are intensified by psychological, physical, financial, social, and performance risks. Lastly, constructed invasion risks (e.g., receiving targeted advertising) are intensified by psychological and performance risks. It is equally important to note that, although performance risks are sometimes used to intensify risks, in specific data collection risks, they are mainly articulated as an identified risk (e.g., participants are concerned about the city council's performance).

It was found that participants are willing to donate their everyday mobility data to a smart city project. Even when risks are identified, and argued during the conversation, participants mitigated those risks by presenting a set of reasons as to why they would still donate data despite those risks. The data analysed showed that individuals seek to mitigate the risks of donating their everyday data should they believe that donating their data would help them avoid certain risks (e.g., being kidnapped), or that it would help improve their lives (e.g., save time during their commute). Risks pertaining to data collection and data processing were mitigated by the same categories: saving time, financial benefits, physical safety, psychological, social, and performance aspects. Risks pertaining to data dissemination were mitigated by saving time and financial benefits. Lastly, risks pertaining to the invasion stage were mitigated by the possibility of from these risks deriving financial benefits.

Regarding the performance category, it often appears as an initially identified risk. This may be due to the fact that individuals, when giving their personal data to the city council, are trusting that entity to act in their best interest. Thus, if a person understands that there may be a performance risk when donating their personal data, then it may create a barrier to donation. This aspect would be connected with institutional trust and how this may impact the intentions to donate. Section 7.6 calls for research to be done in this respect.

The diagrams below illustrate the risk interplay observed in the analysis of the data and analysed throughout this chapter.

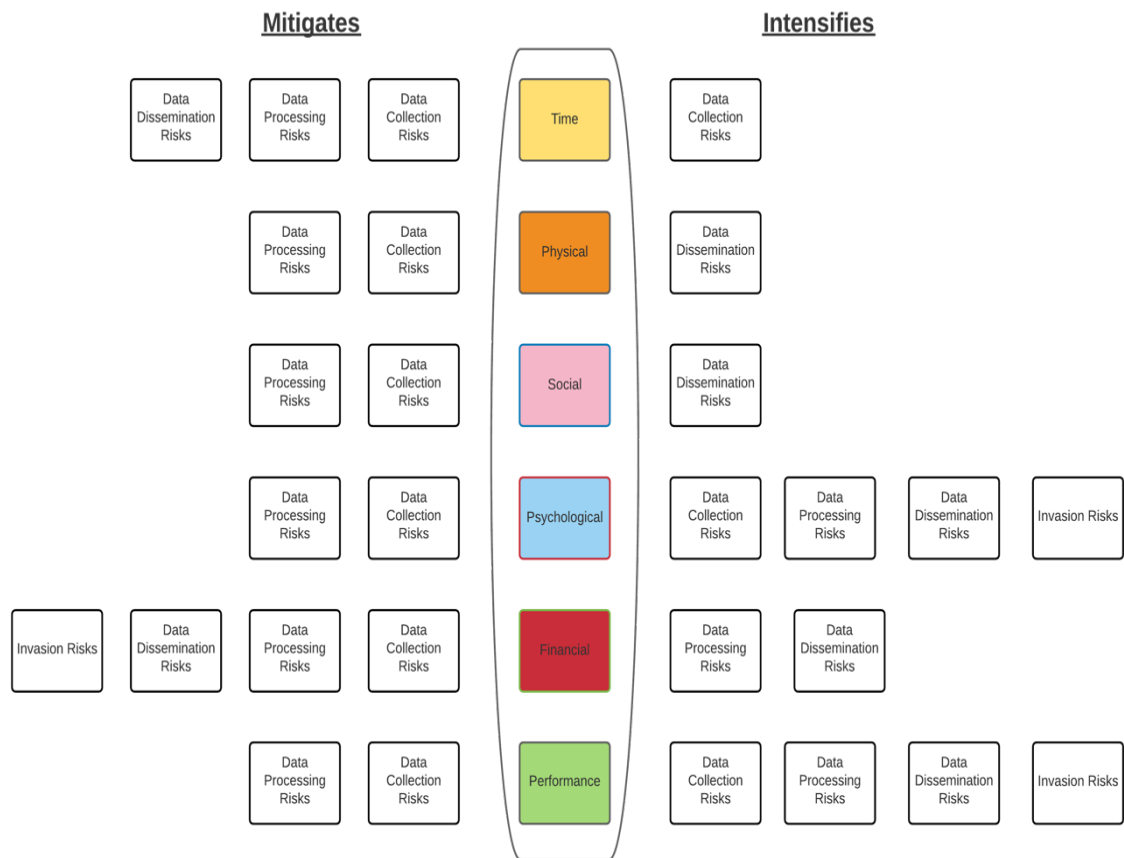


Figure 8 - Risk Interplay

It is worth noting that the performance, financial, and psychological categories are the most prevalent categories intensifying and mitigating risks. Financial benefits were the most used arguments to mitigate every identified risks. Whereas, in the specific case of risk intensification, psychological and performance arguments were the most commonly used across the different identified risks. These observations underline that not only personal but institutional features influence how individuals construct the risks of donating their everyday data to a smart city project. Whilst personal features go beyond a simple trade-off between benefits and risks of donating data, institutional dimensions and trust processes associated with it may influence how citizens think. Although this is not the focus of this research, it is a finding that warrants further investigation. As such, it is mentioned in section 7.6.

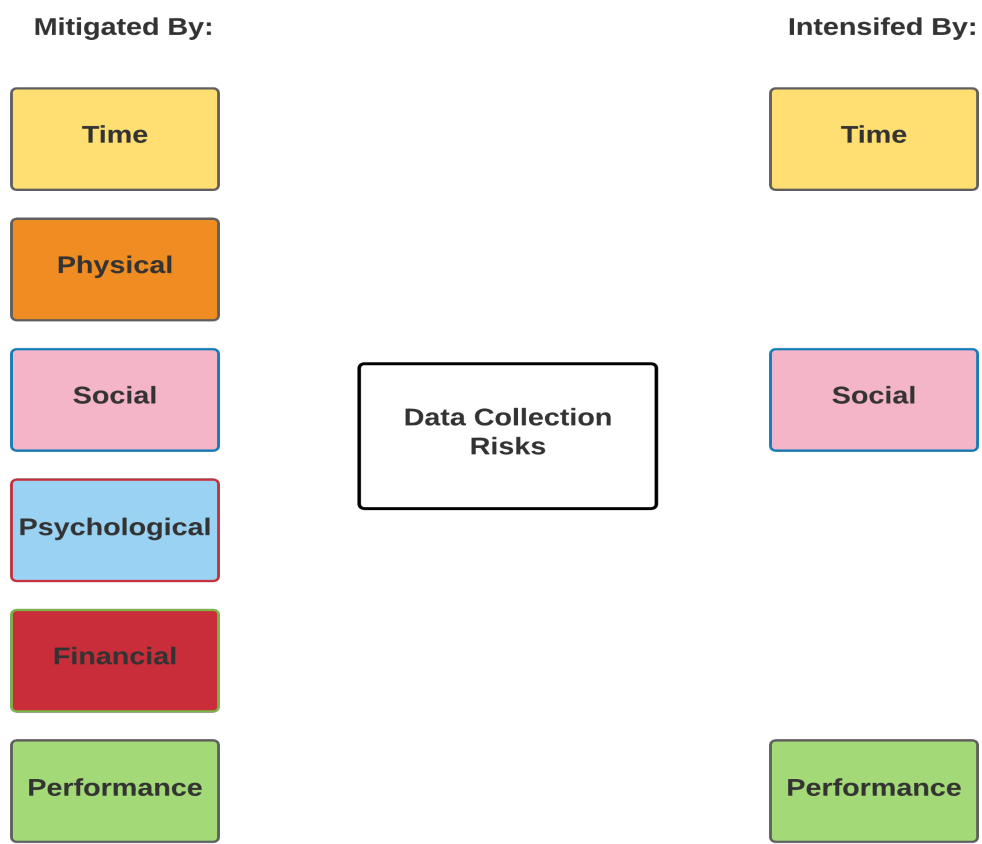


Figure 9 - Data Collection Risks Interplay

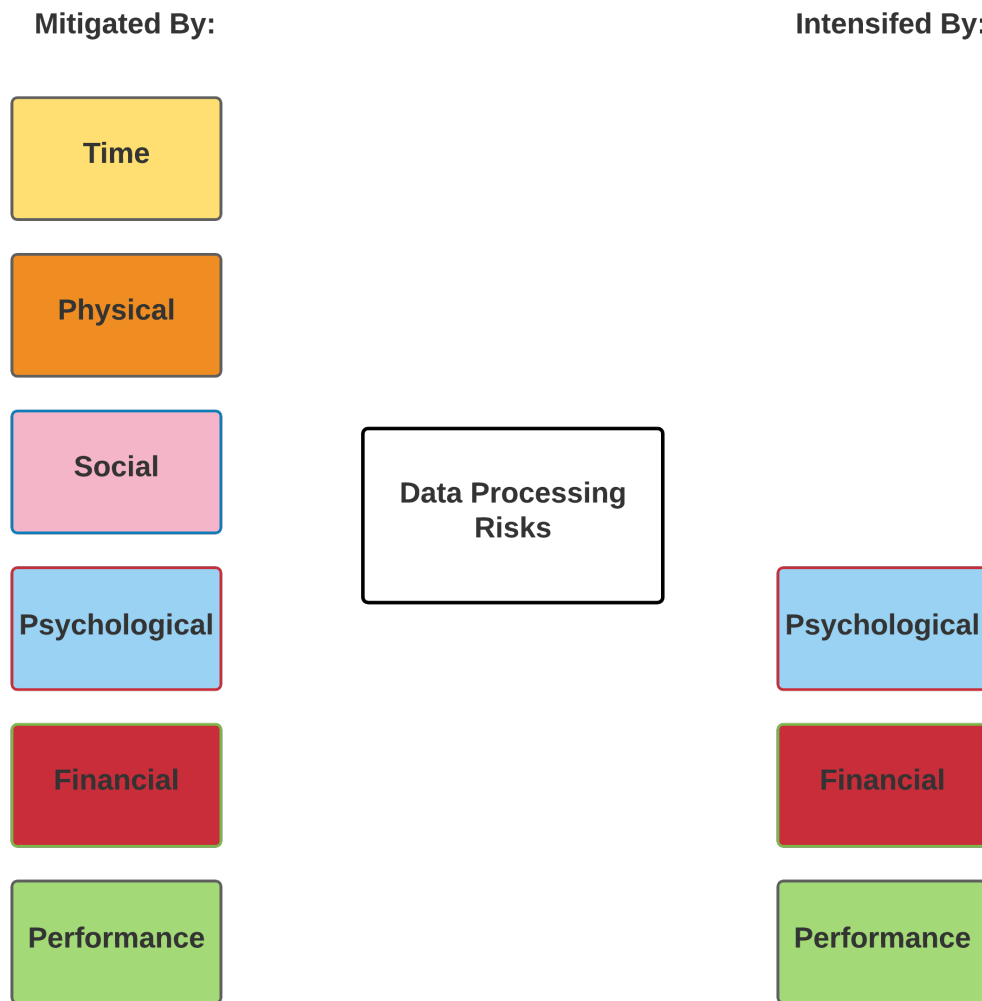


Figure 10 - Data Processing Risks Interplay

Figures 8 and 9 illustrate the data collection and processing risk interplay. Both data collection and data processing risks are mitigated by the same categories of arguments, as previously mentioned in section 6.3.3. However, the only type of argument that intensifies both data collection and processing risks is the performance argument. Arguments pertaining time and social aspects intensify the identified data collection risks. Whereas psychological and financial arguments intensify data processing risks.

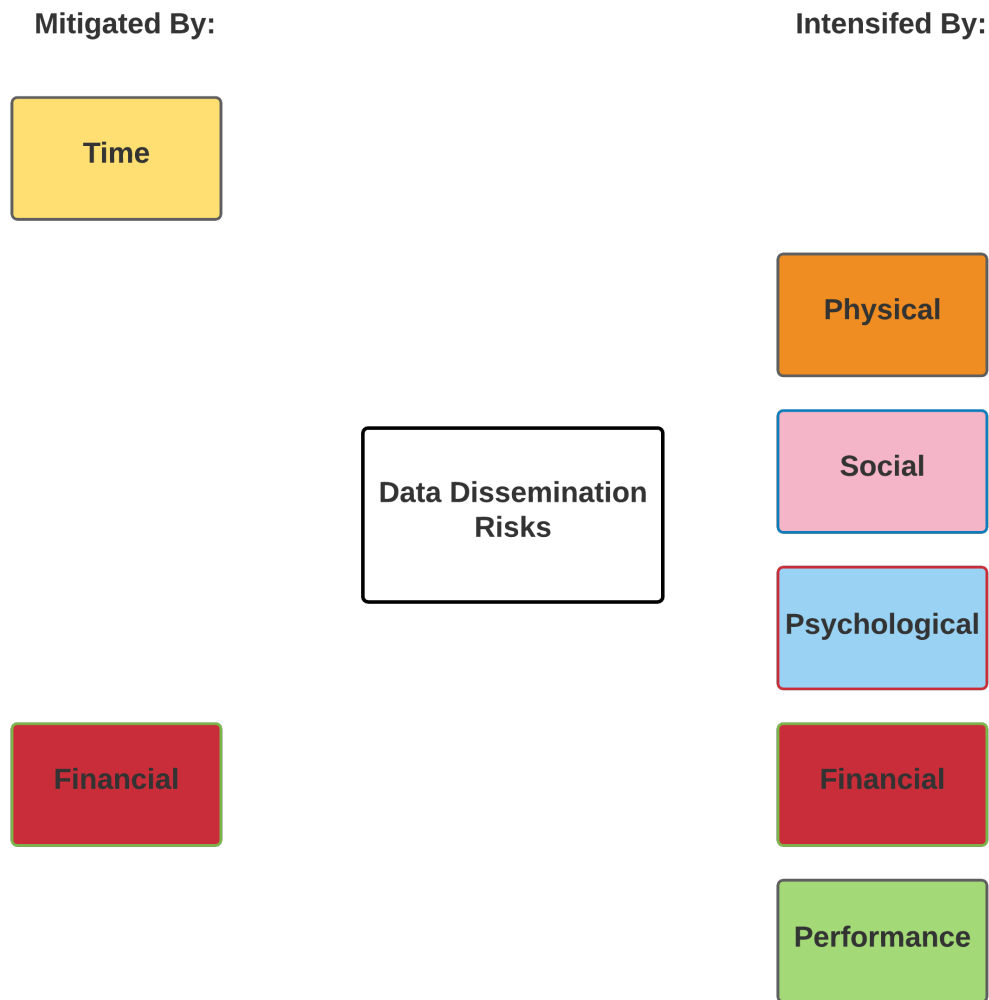


Figure 11 - Data Dissemination Risk Interplay

In regard to data dissemination risks only time and financial arguments mitigate these. However, this identified risk is intensified by five types of arguments, the largest number of arguments intensifying an initially identified risk. Physical, social, psychological, financial, and performance arguments intensify data dissemination risks.

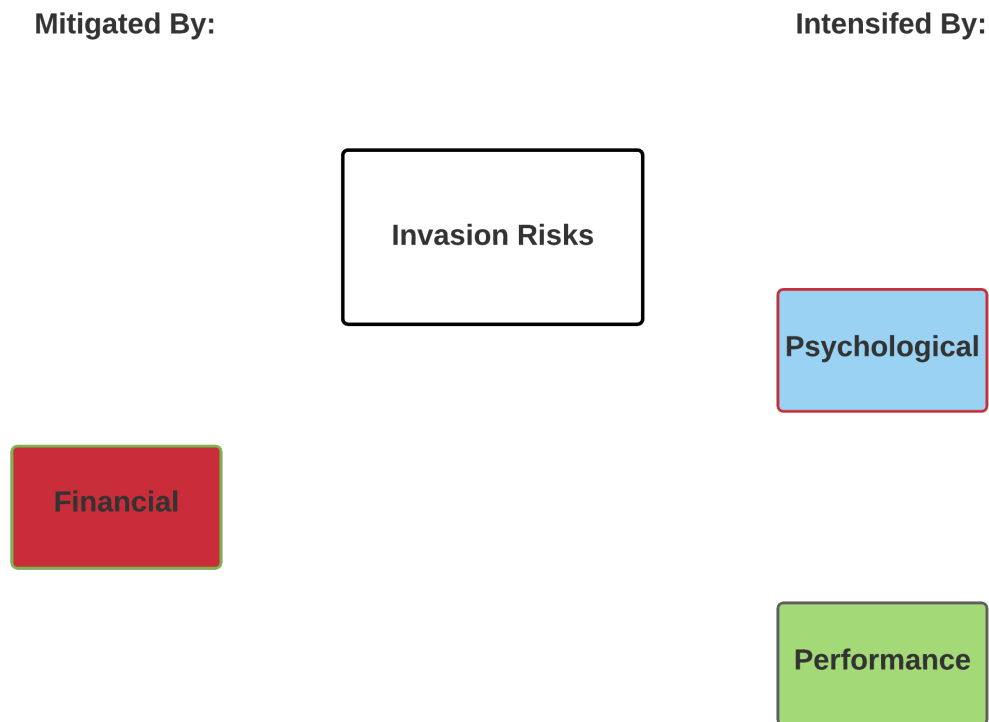


Figure 12 - Invasion Risk Interplay

Lastly, invasion risks are only mitigated by financial arguments, and intensified by psychological and performance arguments. Section 7.6 calls for research to be made to uncover the reasons as to why particular traditional categories of risk latch on to specific categories of privacy harms.

The next section explores how the findings of this thesis relate to the literature and expands on the theoretical and empirical contributions made.

Chapter 7: DISCUSSION

7.1 INTRODUCTION

This research transformed the phenomenon of data donation from being solely focused on, and associated with, medical research and the advancement of knowledge, to be a more overarching and embracing concept. It is the first to define and theorise everyday data donation and investigate it as a separate concept. Specifically, this study focused on exploring the phenomenon of everyday data donation in the context of a smart city. It focused on how individuals construct risks associated with giving their location and mobility data to a local smart city project. It looks at the potential interplay between constructed risks, particularly that of privacy when compared to the traditional risks of donation. It does so by looking at how the participants discussed scenarios surrounding the different situations an individual may encounter when donating data – what risks were constructed, if and how these risks were intensified and mitigated during the course of the argumentation.

Ten focus groups were conducted to explore data donation in a smart city context and the analysis of the observed argumentative risk patterns has been discussed throughout the last chapter. This chapter discusses the extent to which the analysis has answered the research question, its empirical contribution and, and this thesis' various contributions to donation and privacy scholarship. Furthermore, this chapter discusses the research's limitations and by proposing an agenda for future research. The latter

suggests topics warranting further investigation that this thesis has uncovered or briefly touched but that were not the focus of this research. Lastly, this chapter concludes this thesis by concisely drawing the main conclusions and contributions of this thesis.

7.2 EMPIRICAL CONTRIBUTION

The study undertaken in this thesis addresses the following question: ***In the context of a smart city, to what extent are individuals' constructions of the privacy risks associated with mobility data donation¹ based on the general risks associated with donation or risks specific to the donation of data itself?*** It was found that in the context of a smart city, individuals' constructions of privacy risks associated with the donation of mobility data are based on a combination of recognised privacy and donation risks, where the latter operate to either mitigate or intensify the former. In *sensu stricto*, this study focuses on the interplay between the risk dimensions, which have been studied in the context of the traditional types of donation (i.e., psychological, physical, social, time, performance, and financial), and the privacy-specific potential harms, as proposed by Solove (2006, 2008). Extensive data analysis of ten focus groups, yielded distinct risk construction patterns which provide a considerable empirical contribution to the current donation, and privacy scholarship.

Altogether, these patterns revealed that individuals, when facing the decision of whether to donate their personal data to a smart city, in the first instance, identify the possible risks based on the privacy-specific risks. In other words, initially, individuals may construct risks related to how their data is collected, processed, the possibility of their data being disseminated without their knowledge or consent, and, lastly, the risk of having their life disturbed by invasions into their privacy, such as unwanted promotional messages from marketers. There are, however, through the process of social interaction, mitigatory and intensification arguments that will seek to downplay or aggravate what was initially seen as a privacy related risk. The ideas expressed in the focus groups' discussions in which the nature of these privacy risks was explored, without exception, drew on the risks identified in the donation literature.

One of the major contributions of this thesis is that it provides a first documented attempt to define the concept of data donation and observe and understand its dynamics. Specifically, how it is different from data sharing, how it is unique from any other types of donation, and how individuals experience and articulate the risks of donating their personal information to a smart city project. All these dynamics, explored in detail throughout the previous chapter, and discussed in this chapter, help advance the understanding of how privacy plays an essential role in data donation, and how this dimension interplays with what we already know about the current dynamics of donation more broadly.

Moreover, the contribution of this thesis is that the risk privacy harms associated with data donation are not constructed as stand-alone harms, in the data analysed. Instead,

they are constructed as a precursor to the harmful consequences associated with that donation, which is always expressed in terms of traditional donation risks. In the view of the participants, the likelihood of those consequences occurring are used as a way of debating and evaluating whether that original privacy risk is mitigated or intensified. Also, individuals mitigate possible privacy risks by picturing scenarios, rooted in the categories discussed by Barkworth and colleagues (2002), based on personal experience or interaction with others, where donating data can be used to improve their lives, or to avoid a possible danger.

For example, a company collecting or processing one's personal information alone does not seem to pose a risk. It is the different potential consequences of these harms associated with the different stages of data processing that become important to the individuals. The arguments related to the potential consequences fall within the traditional donation risk literature (e.g., Barkworth et al., 2002). For example, should they construct positive consequences from data processing, such as saving time during a commute, then the risk may be mitigated (i.e., the individual may choose to donate). Conversely, should negative consequences be perceived, such as the possibility of being denied health insurance, then the risk may be intensified. These consequences are constructed in reference to the Barkworth and colleagues' (2002) framework.

Nonetheless, these interplays are not universal: not every dimension from the traditional framework intensifies and / or mitigates an identified data processing risk category. Particular privacy risks are intensified or mitigated by a specific set of

traditional arguments. The interplay observed is thoroughly analysed in Chapter 6 and pictured in figure 7.

Furthermore, this study introduces and paves the way for the research of data donation beyond medical data, into the context of everyday lives. By moving past the narrow scope of medical data donation, which has been the subject of data donation research so far, this study is the first to define and examine the concept of data donation in an everyday setting. This thesis also provides a first account distinction between everyday data donation and data sharing, concepts that, until now, have been amalgamated into one: 'data sharing'. Specifically, data donation can be defined as the act, by the data subject, of voluntarily allowing their personal data to be transferred to a third-party that is requesting it, with the objective of promoting public good or for wider social benefit. Data donation differs from data sharing as it is voluntarily given by the data subject, instead of harvested by the third-party, and it is done so with the goal of wider social benefit, whereas the concept of data sharing usually pertains to the commercial use of personal data. The everyday donation of data is especially worth exploring not only because it is an understudied phenomenon, or because it is increasingly practiced by institutions and individuals, but also because of its importance to cities, and implications that it may bring to citizens, both positive (e.g., holding the city council accountable), and negative (e.g., potential privacy harms and consequences).

The theoretical and policy related significance of these observations are now considered.

7.3 THEORETICAL CONTRIBUTION

This study makes a contribution to the theoretical knowledge in both donation and privacy scholarship. These contributions are explored and discussed throughout the sections below.

7.3.1 DATA AND DONATION

This study expanded the conceptual terrain of data donation. Unlike other research to date, this study places data donation in the context of everyday lives. Moreover, this research reveals a wider range of rationales behind one's decision to donate their personal data - there are a number of reasons covered in chapter two. However, a much wider range of reasons were uncovered during this research. For instance, holding the city council accountable for the conditions of the public road, receiving feedback about one's health, being able to track their loved ones, amongst other things are often argued as reasons to dismiss the possible constructed risks and donate. Furthermore, these research's findings both confirm and extend existing research into the constructed risks associated with donation explored by Barkworth and colleagues (2002).

This thesis was largely based on Barkworth and colleagues' donation risk framework. It specifically focuses on their 2002 study that found that the willingness and frequency of blood donations depend on individuals' perceptions of certain categories of risks. These categories of risk were based on Mitchel's (1999) work into risk that

consumers may perceive when deciding whether to try novel products. This framework, however, was proposed as a way to investigate objective risk construction and applied as such by Mitchel and Barkworth and colleagues. However, this thesis stripped these risk categories from their positivist essence and applied them as a priori reference framework for the study of subjective risk through a social constructionist lens. This was the first donation study to take this approach. However, this adaptation is not the only contribution to donation, and Barkworth and colleagues' work. Participants intensify the risks of different data processing stages based on these categories. In other words, data processing indicated the presence of a risk, but it was the consequences beyond data processing which concerned the participants. Furthermore, these intensification arguments were based on the perception of possible unwanted consequences or losses, and on the uncertainty in the occurrence of these consequences. Traditional risk dimensions were, therefore, consistently argued as consequences. Furthermore, they also operate in tandem with other risks, such as privacy risks.

Although notably absent from Barkworth and colleagues' (2002) work, it was demonstrated that there is a privacy dimension to be considered in the study of data donation. This research evaluated data donation risks using a framework derived from the donation literature, situating the data donation risks within that literature. Furthermore, privacy as a new dimension to these risks was added and explored accordingly, almost as if it was an extra layer. Could other types of donation also warrant a consideration of a privacy dimension when studying how individuals construct the risk of donating their personal data? I argue that yes. Nowadays, and as

time goes by, technology innovates, empowers, enables, and mediates even the most basic of human tasks and transactions⁴². Donation is not an exception. For instance, genetic data can be stolen from direct-to-consumer genetic testing⁴³; Blood can be used to build genetic databases⁴⁴. There may be different ways in which a privacy dimension is present, especially when technology, particularly that which is capable of surveilling individuals and groups, is prevalent in almost everything people do.

Moreover, in chapter two, this research adopted the notion of impure altruism. In essence, impure altruism asserts that individuals experience a sense of satisfaction and joy after helping others. As George Bernard Shaw (1896, pp. 387) famously argued: “a millionaire does not really care whether his money does good or not, provided he finds his conscience eased and his social status improved by giving it away”. With this argument, one may think that impure altruism is not only related with psychological rewards (i.e., intrinsic - feeling good) but also with social rewards (i.e., extrinsic - increase in reputation). Although a faint notion of altruism is present in this study, as discussed in the last chapter, there is a strong trade-off logic (i.e., ‘is there something in it for me?’) present in the participants’ narrative. This trade-off narrative may lead to an oversimplification of what is a very complex phenomenon influenced not only by individual experiences, but also by institutions, social environment, and social actors and events. This pattern of interplay between mitigation and intensification of

⁴² For example, “Amazon Prime Delivery Fleet gets FAA approval” (see <https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html>)

⁴³ <https://www.consumerreports.org/health-privacy/your-genetic-data-isnt-safe-direct-to-consumer-genetic-testing/>

⁴⁴ <https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html>

risks, especially when individuals seem to be willing to donate their personal data in exchange for a personal benefit, contributes to the understanding of impure altruism, supporting Andreoni's (1989, 1990) and others' argument.

Additionally, it is important to note that the 'what's in it for me?' argument may not refer to a trade-off notion, but, instead, be a representation of the participants social identity. Here, the 'me' they are referring to could be to one of the multiple levels of the social selves. In other words, they could be referring to 'me' as a cyclist, Milton Keynes residents, environmentalists, parents, amongst any other group they feel part of. Therefore, as discussed when this thesis explored the idea behind social identity in section 3.3.2, willingness to help by donating their personal data may be a reflection of in-group helping. For example, in order to help their fellow cyclists avoid potential dangers on the road, such as glass, potholes, amongst others).

7.3.2 PRIVACY

After discussing the theoretical contribution to donation studies, it is now essential to look at the theoretical contribution to privacy scholarship. This research has shown how the construction of privacy risks is rich in social elements. Thus, it offers support for a conceptualisation of privacy that shies away from being individual-centric to being of key importance to the integrity of a society.

7.3.2.1 THE TAXONOMY OF PRIVACY HARMS AND DATA

DONATION

One of the theoretical underpinnings of this study was Solove's (2006, 2008) privacy harms framework. Solove's comprehensive framework displays the plethora of ways that individuals' privacy may be violated. These categories present the five stages of the data processing that endanger an individual's privacy: information collection, processing, dissemination and invasion. Within each stage, there are several different ways how information can be misused (see section 3.5.1).

In spite of the fact that Solove's framework is intended as a legal framework that aims to categorise what may constitute privacy violations, this study investigated whether individuals perceived them as what they were conceived to be – privacy harms – and how they interplayed with the traditional dimensions of donation risks set out in the donation literature. This is the first study that applies a privacy framework to a donation context. Similarly, it is one of the first scholarly instances aiming to adopt Solove's taxonomy to support the investigation of social constructions of risk. Accordingly, first, Solove's taxonomy extends beyond the realm of legal scholarship. The empirical work has demonstrated how the different privacy harms have meaning in different everyday settings. Individuals can certainly identify the main categories of harm that Solove sets out in his framework. Although the participants do not always mention all of the specific examples introduced by Solove, they discuss the broad categories of data processing.

Second, from this initial identification of risk, the intensification of risk is then discussed by using the traditional risk framework. However, these are not universal within the four data processing stages. Each stage seems to have a given set of arguments intensifying it. For instance, at the data collection stage identified risks can be intensified should individuals perceive that from these can occur any psychological or time risk. For example, participants can argue that the process of donating data can take too much time or be too complex (i.e., time risk) and, equally, they can be concerned about the wealth of information being collected and what that may say about them (psychological risk). At the data processing stage, individuals may intensify identified risks should they perceive financial or psychological consequences. For example, whether the processing of the data they donated may exclude them or aggravate their premiums from given services (i.e., financial risk), and what would people think of them after processing their data (e.g. “should cycle more because...” – psychological consequence). At the data dissemination stage, several consequences may be used to intensify this identified privacy risk: psychological, physical, financial, and social risks. In specific, if the city council passed their data to a third party what could the consequences be in all these domains? At the invasion stage, only psychological consequences were used to intensify the risk. For example, should the participants receive promotional [spam] e-mail for a dietary product, they would feel overweight and, thus, experience psychological consequences of this risk.

Furthermore, the findings of this thesis also support Kitkowska and colleagues’ (2018, pp. 59) argument that individuals experience “privacy harms as generic and simplified models, not individually as suggested in Solove’s framework”. As continuously

argued, data processing stages, and harms (e.g., disclosure) do not represent constructed risks by themselves. It is the consequences that do so. For example, disseminating one's data by selling it to a third party, only is constructed as a risk if negative consequences derive from this act.

Moreover, it has been demonstrated that the privacy harms identified by Solove can be mitigated in an everyday setting using the traditional donation risks framework set out by Barkworth and colleagues. Equally, there is a variation of mitigatory arguments depending on the stage of data processing being discussed. At the data collection and data processing stages, these risks could be mitigated if that could improve participants' lives (e.g. saving time commuting), improve their financial life (e.g. receive discounts), protect them against physical or psychological harms (e.g. be able to quickly locate family members should they be in any danger), if the programme was widely accepted or if it would increase their social status, and, lastly, if participating in this programme means keeping the city council accountable. At the data dissemination stage, participants focused on discussing possible financial benefits. For example, if their insurer could have access to their data, they could, perhaps, receive a discount in their premium. In the invasion stage, individuals mitigated the risk by arguing that they would welcome unsolicited communications should these help them financially. For example, coupons for products they want.

Can Solove account for these patterns and nuances of human perception? In short, no. Solove (2006, pp. 558) attempts to "provide a clearer and more robust account of privacy – one that provides us with a framework for understanding privacy problems".

He argues that the justice system and policymakers are ill-equipped to identify privacy problems. That activities that impact one's privacy often may not be "socially undesirable or worthy of sanction", thus making privacy such a complex issue. This is the aim of his privacy harms framework: to provide a clearer picture of how privacy violations arise and how individual's privacy may be violated. Indeed, this study has shown that individuals perceive all these categories of data processing as potential risks to their privacy. However, and the most striking finding is that these privacy specific harms alone do not construct the risk of donating personal data. Instead, it is the possible consequences, positive or negative, of these data processing stages that influence the individual's judgement.

Here, and throughout this study's narrative, and that of the participants there is a strong trade-off logic. This may result in incurring the risk of giving this phenomenon an oversimplistic perception to the reader. This trade-off logic, or, in other words, the argument of privacy as economic rationality has been thoroughly debunked. Here, often "information is modelled as a commodity that can be traded" (Dourish and Anderson, 2006, pp. 326). However, as seen throughout this study, as discussed below, and as brilliantly argued by Dourish and Anderson (2006, pp. 327) "economic models fail to recognise that privacy is, essentially, a social practice. [...] Privacy is not simply a way that information is managed but how social relations are managed". Below this thesis contribution to the conceptualisation of privacy as a social value is discussed.

7.3.2.2 THE SOCIAL VALUE OF PRIVACY IN DATA DONATION

Chapter three set out that in order to conceive the social value of privacy, one has first to move beyond the narrow focus of legal scholarship in privacy and focus on the current thinking of privacy as individual-centric, and as a boundary between individuals, and between individuals and the state (see Regan, 1995; Steeves, 2009; Raab, 2012). Essentially, these scholars argue that privacy exists beyond the individual level, at a group and society level. Privacy's social value is about an individual's self-determination and autonomy. It is what allows individuals to interact, in a myriad of social roles, with other people and groups. As Steeves' (2009, pp. 205) eloquently puts it "privacy is what enables the self to see itself as a social object and to negotiate appropriate levels of openness and closedness to others". Moreover, privacy is about the effect of that interaction on the social fabric. In other words, privacy, as experienced by individuals, is embedded in social norms governing how we interact with each other and with institutions. Accordingly, if privacy is systematically violated, not only is this harmful for the individual's self-determination and autonomy but also for the integrity of a fair and democratic society.

In this study, components of this social value were entrenched in how individuals constructed the risks which arose as they considered donating their data. As such, participants mitigate data processing risks when, from these, they cannot possibly conceive any sort of consequences or when it constitutes an improvement to their lives. These can be interpreted in two ways: for once, the deleterious impact donating data may have on their social life and relationships, and thus in the quality of their life. And

second, data donation may present a potential for new opportunities to foster relationships and increase their own social standing. For instance, the act of donation is often perceived as ‘altruistic’ by others. Therefore, the participant donating their data and discussing it may be seen as an ‘altruistic’ individual, thus potentially increasing their social standing with their peers.

Furthermore, it is also evident the influence different social roles play on an individual’s construction of privacy harms. The argumentation patterns vary according to the perceived social role in a given scenario (e.g., Kris as a banker vs mother vs wife). Accordingly, the pattern observed does not represent an individual-centric notion of privacy. If that was the case, instead of observing highly contextual, role-specific risk perception patterns, one would, perhaps, observe a perception of the risk at the data processing stages. However, that is not what happens. The data processing stages, as per Solove’s framework, does not construct risks by themselves. Instead, it is the possible consequences of the data process that individuals perceive as risks, whether those are upstream or downstream that construct the risk of data donation; these help determine an individual’s inclination towards donating their personal data.

Moreover, the individuals’ willingness to participate in the smart city project by donating their personal data clearly demonstrates some elements of the social value of privacy. Specifically, the participants look to negotiate under what terms the data is processed and seek to mitigate possible consequences. This willingness to participate on a project of this kind, while trying to remain free from surveillance in other domains of their [social] lives, such as driving behaviour, political inclinations, and religious

activities, demonstrates the social value that privacy holds to individuals. In other words, the patterns observed show that people believe that some consequences may derive from being surveilled beyond the initially intended and agreed purpose (e.g., insurance premium raise, what are they doing with their friends, creating psychological unease), and, thus, using mitigation arguments, they try to negotiate and be assured that their expected boundaries are being respected.

Nonetheless, the patterns identified do not offer enough information to support privacy as being important for individuation (the process of identity formation discussed in chapter 3), as Steeves (2009) argues. This is not to claim that the findings refute her theory. Simply, this research did not look into individuation, and the patterns observed do not account for a notion of privacy as fundamental for an individual's identity formation process.

7.3.2.3 CONTEXTUAL COMPONENTS IN DATA DONATION

Nissenbaum (2009), in her theory of privacy as contextual integrity, contends that expectations regarding the different stages of data processing are determined by the social norms of a given context. Therefore, individuals expect their data to have a legitimate flow appropriate to the relevant context. For example, in the context of a visit to the doctor an individual can expect that only their medical data and other relevant information be processed by the doctor. There is an appropriate flow of information to the patient to the doctor and healthcare system that one expects not to

be shared or used elsewhere. If that is the case, then it would constitute a privacy violation.

In the context of a smart city should an individual decide to donate their data, they may expect their information to be collected and processed by the city council only for the purposes that were previously agreed – in this case to improve mobility within the city. In this specific case, an individual donates their personal and mobility data to a smart city with the objective of helping to improve the city's road networks, public transportation, and other mobility-related systems. Furthermore, the context was focused on cycling-specific activities (i.e. commuting or pleasure cycling). This was the context under what the participants were discussing data donation. Accordingly, and in line with Nissenbaum's theory of privacy as contextual integrity, should the city council use the data for something else other than what was expected by the participants, it constitutes a privacy violation. This violation may be a nuanced use of their data, such as, for example, the collection of any mobility data besides cycle-specific activities, or to aid the research of sociodemographic clusters in the city, or something more draconian as, for example, disseminating driving behaviour data to insurance companies.

Furthermore, as discussed in chapter three, Nissenbaum (2009) proposes four key parameters to conceptualise context-relative information norms: *contexts* refer to the situations in which the transfer of information occurs; *actors* refer to the parties involved in the flow of information: who sends the information, who is the recipient, and who is the information about (information subject); *attributes* refer to the types of

data being transferred; *transmission principles* refer to the constraints to the flow of information from one actor to the other in a given context (e.g. medical consultation is guided by a set of transmission principles). In the context of the donation of personal data to a smart city, the context lies under what circumstances is the data requested (e.g. cycling mobility data); the actors comprise the citizen participating (information sender and subject), and smart city project (information recipient); attributes concern all the personal data pertaining to cycling activities as well as sociodemographic profile of the participant (e.g. speed, itinerary, age); transmission principles are constricted to the conditions under what the participant accepted to be part of the project (e.g. use of data only for planning and improvement of road networks).

The patterns identified in this research support Nissenbaum's framework and provide some detail. First, it was demonstrated that individuals perceive risks differently depending on the data processing stage. This finding supports her argument that privacy protection should be tied up to the informational norms and expectations of specific contexts. Second, although this thesis is focused on a smart city context, individuals rushed to imagine other contexts where they would intensify or mitigate a given data processing risk. Accordingly, it is not the technology, nor the fact that the data is being given to an institution, that constructs the perceived risk but indeed the informational norms perceived by the donor. Third, it was also demonstrated that even if the informational norms are violated by the institution, it does not exactly result in a negative reaction by the individual. Instead, it is the consequences of that violation, and their severity, that determine whether the risk is intensified or mitigated. Therefore, even if contextual norms are broken, one has first to understand the consequences of that violation. The author agrees that for privacy to be deemed as

violated it does not have to be perceived as such by the subject of that violation. However, it is vital to add this subjective dimension to privacy scholarship where one has not to look only into whether or not norms were broken, but also to the ensuing consequences.

For instance, imagine an individual engaging with a smart city project by agreeing to donate their commuting data (i.e. where they expect the data collected to be his location only during the commute). Should the individual perceive that the smart city may collect more than mobility data, and start collecting the individual's heart rate data, as per Nissenbaum's theory it would constitute a privacy breach from that individual's point of view. However, to the individual it may or may not be deemed as such – it all depends on the consequences of the data breach. The individual, at a first instance, would identify a data collection risk in tandem with a performance risk (i.e. the city council is not performing as it was expected). Nonetheless, if the individual perceives a negative consequence of the city council having their heart rate data (e.g. discomfort in knowing that the city council is aware of their fitness levels), then the initial data collection risk is intensified. Conversely, if no negative consequences are perceived, or even if an improvement of their life is perceived (e.g. the data donation app provides feedback on their fitness efforts during their commute), then there is place to a mitigation of the data collection risk. In sum, although the informational norms of this context were violated, the individual's perception is dependent on the consequences to their life.

7.4 OTHER OBSERVATIONS

7.4.1 BOUNDARY NEGOTIATIONS AND RELATIONSHIP DEVELOPMENTS IN DATA DONATION

Altman claims that privacy is at the heart of complex social interactions, in which individuals and groups seek a balance between being open and closed to interactions in order to achieve their ideal privacy levels. In order to reach these ideal privacy levels, individuals and groups negotiate their boundaries. In fact, Altman defines privacy as the “selective control of access to the self” (Altman, 1975, pp. 24).

The patterns identified in this study demonstrate the attempt from participants to negotiate boundaries and selectively control the access to their information. In essence, that is what can be observed when individuals try to mitigate the privacy-specific risks. The participants would be willing to donate their personal data and engage with a smart city under their own terms. It becomes important to individuals to be aware of what exactly will happen to their information once it is donated (e.g., how safe is it going to be? How much will they know about my routine?). Even if negative consequences are perceived, the decision to donate data is not immediately dismissed, instead, mitigatory arguments are often still proposed and discussed. If elements of a dynamic boundary negotiation were not present, as, for example, Westin’s “social withdrawal” argument does not account for, then individuals would perceive the risks at the privacy-level. This is simply because just donating data, without the opportunity to

selectively inquire the donation process and the possible consequences, would constitute, in essence, a violation of privacy. That is not to say that Westin's theory does not account for the individuals attempt to achieve an ideal level of privacy, on the contrary, Westin's argument specifies exactly that, however, they only can do so by withdrawing from their social lives.

Petronio (2002, pp.3), largely based on Altman's theory, suggests that "privacy boundaries are coordinated between and among individuals" allowing for a better understanding of the tensions in deciding whether or not to disclose private information. Petronio's (2002) CPM theory, as discussed in chapter three, is supported by three main principles that guide individuals' privacy choices. First, individuals assume they have ownership of their private information. This belief helps them devise boundaries more clearly, thus allowing them to grant, or not, others access. This perceived control over their own information leads to the second principle: privacy regulation. This contends that individuals set up their own privacy rules as a way to regulate the flow of their private information. In consequence, if an individual discloses their information to others, they expect the third parties, that now became co-owners of said information, abide by the original owner's rules: "original owners see the recipient having fiduciary responsibilities for the disclosed information" (Thompson, Petronio and Braithwaite, 2012, pp.57). The last principle refers to the phenomenon that occurs when recipients of private information do not know or conform to the privacy rules expected by the owner. According to Petronio (2002), this coordination between and amongst individuals, and the responsibilities they share

as information co-owners enable the development of [social] relationships. Therefore, privacy is essential to establish and cultivate relationships.

This research fully supports Petronio's principles: Individuals understand that their data is their property, and thus are in charge to decide whether or not to donate. In fact, that is one of the premises upon which the concept of donation, and as a consequence, data donation, is built upon: individuals or groups transfer their property to other individuals or groups. Furthermore, due to the unique characteristics of data (e.g., shareability), discussed in chapter two, section 2.2.7, transferring ownership of data may be a complicated endeavour, therefore, smart-city projects and citizens alike become co-owners of personal information. Nonetheless, individuals still require that e-governments abide by their expectations regarding how their data should be processed. That is visible by how the patterns in the interplay of risk perceptions occur: should individuals perceive negative consequences may occur from the different data processing stages, then the risk is intensified, and individuals become more resistant to donate.

Moreover, individuals in this research form different types of boundaries. First, and perhaps the most distinct boundary, is the need to separate government, and the non-profit use of one's data, from the companies, and consequently for-profit use of their personal information. This is where the performance risk becomes evident: when individuals perceive that the city council may not perform as they expect (e.g. by protecting their donated data, by selling it, by using it for other activities other than what was initially consented). Thus, for instance, the need for the individuals to be

reassured of the non-profit use of their data. Should the smart city project not conform to the norms expected by the data donor, then, in congruence with Petronio, there is place to, what she calls, privacy turbulence (i.e. when there is a failure from one of the co-owners of the information to hold the rules as expected).

Nonetheless, it is not possible to ascertain whether donating data, or the perceptions of the risks involved in doing so has any implications to the development of interpersonal relationships, as Petronio contends. It is theoretically possible that should all three principles be met by the donor and smart city project, as it is asserted, along the donation process then a relationship may be fostered. Yet, this and other factors relating to the development of relationships between citizens and smart cities, in connection to data donation, such as, for example, trust, are not the objective of this study, and, thus, should be left for a future research.

7.5 RESEARCH LIMITATIONS

The study conducted contributes theoretically and empirically to the understanding of how risks associated with data may be constructed by the individual. The research focused on individuals aged 35 to 49, living in, or commuting to, Milton Keynes, that cycled on a regular basis for commuting or leisure purposes, thus not being yet clear how this research would apply beyond this setting. Moreover, the age range of this group means that they have some knowledge of new technologies, however, they tend to be not as involved as younger generations. This may, for some, lead to a lack of

understanding of the potential nefarious [privacy-related] consequences of new technologies, and to others, it may lead to a more closed approach towards the use of technological tools.

Furthermore, there were a very reduced number of individuals belonging to ethnic minorities represented in any of the focus groups. There was some difficulty from the recruitment agency employed to recruit a diverse sample. According to the person responsible for the recruitment of participants to this project, the difficulty to recruit from marginalised groups may stem from the somewhat narrow sampling characteristics (i.e., age range, gender and interest in cycling in and around Milton Keynes) and the need for a high number of participants.

Furthermore, the use of qualitative methods, such as focus groups interviews, present some limitations. It ought to be acknowledged that participants, despite how engaged they may be in a discussion, might not express their honest opinions, particularly if they disagree with others. In consequence, some focus groups may be influenced by more dominant participants restraining others from feeling comfortable in expressing their own opinions. Additionally, the introduction of scenarios and questions that serve as guidance and elicitors of discussion may potentially influence participants' responses. Reflecting on the structure of the focus groups, and the way they were conducted, it may have been beneficial to allow participants to, at a first instance, share their arguments and engage in a free-of-constructs discussion related to data donation in a smart city context, before presenting the scenarios devised.

The employment of focus groups does not allow for a generalisation of results, nor for the inference of causality between constructs. However, as argued in chapter four, it is well established that how individuals understand risk is subjective and socially constructed; although, as with many other disciplines, philosophical differences may occur between researchers. Furthermore, this research observed phenomena in line with the different theorists discussed, confirming and adding to what they have done as explored throughout this chapter. According to my research philosophy, and the research question being addressed, the use of focus groups is an appropriate research method to be employed. The use of focus groups enables and foments the interaction between participants, allowing for different opinions to be shared, giving place to a rich interplay of arguments and examples that help uncover different behavioural and argumentative patterns. A critical interpretation and explanation of these patterns aids the understanding of the phenomena being studied.

Lastly, the analysis of the data did not offer support to crucial cornerstone conceptualisations of privacy as, for instance, it being central for individuation or even for relationship-making. Although not the objective of this research, no support for these concepts was observed in the data. This may be simply due to the fact that the focus groups' discussions were not conducted in a way as to elicit argumentative patterns that could be explored in a way to investigate these concepts in the context of data donation.

After discussing the limitations of this study, the section below suggests some future research directions that may be explored. These research directions derived from

different topics that arose during the analysis of the data that are not directly related with the aim of this thesis, although they are pressing issues that warrant further investigation. Furthermore, they help furthering the understanding of data donation, and, in specific, how different issues impact individuals' perceptions of the risks involved in donating their personal data.

7.6 FUTURE RESEARCH DIRECTIONS

This research has focused on understanding how individuals construct the risks of donating their personal mobility data to a smart city project. It suggested a framework for the exploration of risk perception in data donation, and empirically tested it in the context of smart cities, in a given geographical location and age group. During the development of the conceptual framework and analysis of the empirical data, several themes adjacent to this research, were constructed. Therefore, the conceptual framework proposed, and wealth of data created by focus groups discussions, warrant an exploration of how the construction of data donation risk vary between social roles (e.g., how the same individual in different roles perceives the same scenario – mother vs professor vs wife).

Furthermore, how individuals make sense of a more complex disclosure scenario and how their constructions of risk vary within these more complex scenarios warrants further investigation. The importance of exploring this phenomenon in the particular context of data donation centres around the fact that sensemaking is, according to

Weick, Sutcliffe, and Obstfeld (2005, pp. 409), “the primary site where meanings materialize that inform and constrain identity and actions”. A closer at how individuals assign meaning to data donation risks and consequences in more complex scenarios is needed.

Another narrative present throughout the focus groups discussions was on whether the participants trusted the city council in order to give them their personal data. The trust in institutional bodies seems to play an important role on an individual’s decision on whether to donate their personal data. This research found that there are personal and institutional aspects influencing individuals’ decisions to donate their personal data (argued in section 6.4). This institutional dimension influences how individuals think and construct the risks of donating personal data. Research has recently started to address the trustworthiness of public authorities in security contexts (e.g., Ball et al., 2018). Future research ought to further investigate the dynamic institutional trust plays in individuals’ perception of risk in the specific context of data donation to an institutional body (e.g., city council).

In the context of data donation, decision-making is yet another domain that demands further exploration. This thesis focused only on how individuals construct risks, and the dynamics between identification, intensification, and mitigation of risks. However, it did not evaluate how these constructions impact the individuals’ decision-making process. Indeed, mitigatory arguments seemed to make the potential issues involved with donating data bearable and acceptable, however, this impact in decision-making was not evaluated. Further psychological studies are warranted.

Cultural variation may influence how individuals construct the risk of donating their personal data. An already well-developed topic in privacy scholarship has argued that culture influences how individuals understand and experience privacy (see Zabihzadeh et al., 2019; Merhi et al., 2019). Moreover, including a more diverse sampling, including marginalised groups, could yield different results. Also, gender may be another factor influencing how individuals experience the risks of donating their data. Studies have established how different genders experience privacy violations differently (see Tifferet, 2019; Ball et al., 2012; Friedman et al., 2006). Further research is needed into how these, and other sociodemographic factors influence how individuals construct the risk of donating their personal data.

Furthermore, this research focused on the donation of mobility data to a smart city. The donation of other types of data (e.g., biometric data, thoughts and feelings data) may yield different constructions of risk. Similarly, a different focus on where personal data is donated to may return different constructions of risk. As this thesis' focus on the donation of personal data to a smart city, perhaps, other studies can focus the investigation on the donation of data for suicide prevention, for disease prevention (e.g., as can be the case of COVID-19 track and trace programmes), for governmental planning (at a macro level, rather than local). Further research into these could advance the knowledge of how individuals construct the risks of donating personal data in different contexts, and under different norms (e.g., type of data, organisation to which data is donated).

This research has shown that privacy should be considered as an added layer to the donation studied. Privacy-specific harms, and how information flows were shown to impact how individuals experience data donation. Research into traditional donation should acknowledge this privacy dimension and investigate the possible dynamics of this dimension when individuals consider whether to donate a traditional asset (i.e., blood, organs, products, money, time).

Data showed that there are particular categories pertaining to the traditional risk framework that interplay with specific privacy risk categories. This interplay was analysed in chapter six. It was established that there is an intensifying and mitigating relationship between them. However, future research should aim to uncover the reasons why they latch on to each other.

Lastly, while the participants seem to focus on privacy issues, and possible consequences to their lives stemming from these issues, it is important not to forget that data donation is a type of donation. Accordingly, one ought not to look at it through the same lens as one would investigate an act of giving data in exchange for access to a service (i.e., data sharing), as is the case of, for example, any social media platform that monetises their users' personal information. This distinction was thoroughly explained in chapter two. Therefore, future research into data donation should be mindful of the specific characteristics that constitute the fine line between data donation and data sharing. Also, in light of Skatova and colleague's (2014; 2019) work in data donation, as argued in section 7.4.2, it should be noted that academic scholarship investigating data donation has to consider that medical data, and

academic data are just sub-types of data donation, governed by a different set of norms. The contemporary study of data donation has to account for the fact that data can be used in, virtually, any domain of everyday life.

7.7 POLICY IMPLICATIONS

Since starting this research, data donation has significantly expanded. Data donation practices are now being used not only as a ‘one-time’ activity, in extreme circumstances (e.g., personal data from a suicide victim), or for [medical] research purposes, but also as a way for citizens to participate in the planning and development of their city’s policy and infrastructure (e.g., Cardullo and Kitchin, 2019). Smart cities are capitalising on new technologies to involve citizens, and for citizens to hold their cities accountable. Research in smart cities and e-participation is equally expanding (e.g., Webster and Leleux, 2018; Meijer and Bolívar, 2015; Ismagilova et al., 2020). In this section the policy implications of this research’s findings are discussed. This section begins by exploring data protection issues, specifically, the issue of the prioritisation of consent by policymakers and decision-makers. This section then continues by exploring other key players in the smart city ecosystem, the implications of the social value of privacy to smart city policies, and the need to develop inclusive systems that account for how citizens experience the risks of donating their data. These policy recommendations are aimed towards local authorities developing smart city policies and ecosystems, as well as private companies providing the infrastructure and functionality that form the technological basis of a smart city.

The first aspect of policy to be addressed draws upon the breadth of data protection issues that arose in the results. Despite the expansion of data donation and other e-participation initiatives, regulatory and policy bodies concerned with designing privacy legislation have long prioritised the issue of consent, which is generally focused on the way institutions collect data (Mantelero, 2014). Giving consent to data collection, and the ability to withdraw it at any point it is still the main focus of regulators, as if the sole control over the way data is collected is the main concern of individuals and, consequently, the main weapon against privacy incursions. This thesis has shown that data collection is a small part of the regulatory and governance setting that causes concern from the citizens' point of view. Individuals experience risks throughout the process and not only at the data collection stage. Data processing and dissemination risks were intensified by a larger number of traditional categories than data collection. Accordingly, regulators should focus on assuring that not only individuals' privacy is protected throughout the different stages (i.e., data collection, data processing, data dissemination, and invasion) but also that potential consequences to people's lives (i.e., as represented by the traditional donation risk categories) are accounted for. Therefore, regulators are advised to look beyond the 'notice and consent' model, and into the other stages as proposed by this research (ICO, 2017).

Explaining to data subjects what is done with their data before asking them for consent (i.e., 'notice and consent' model) is problematic due to the fact that the majority of individuals lack the technological knowledge necessary to understand how their data will be processed (Buttarelli, 2016). Another criticism is that when asking data

subjects for consent, their options are either to accept or deny (i.e., binary model of consent) for their data to be collected (Nguyen et al., 2013). The problematic of consent is that it only seems to be applicable at the data collection stage. As Nissenbaum (2018) argues, often people do not know what they are consenting to. They are merely presented with a pop-up that asks them to store cookies on their browser. What this really means, the majority of individuals does not know, and the need, or strong desire, to access the website or service (in a timely matter) precludes them from rejecting the cookies. This means that individuals that opt out of having their data collected are denied access to the service they were interested in the first place.

Nissenbaum (ibid) claims that this focus on consent may be harmful by giving people a false sense of control over their personal data. This research calls on those in charge of smart city projects, legislators, and regulators around the world to look beyond the ‘binary’ model of consent, giving data subjects more flexibility to provide informed consent throughout their interaction with the smart city. This would allow individuals to choose when and how consent is given, rather than at the outset. Citizens’ rights need to go beyond the control over their consent, and throughout data processing. Individuals’ rights, privacy expectations, risks and consequences experienced need to be considered during the design of the ICTs. Article 25 of the GDPR states that “the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and

their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons". In other words, institutions must ensure that "only the personal data that is necessary to achieve the purpose of the processing is enabled" (European Data Protection Board, 2019), promoting greater transparency.

Furthermore, this thesis demonstrated how data donation risks are experienced. Specifically, individuals are not only concerned with what is done with their personal data (e.g., the issue of consent or how their data is collected or processed), but also, the consequences experienced by them (e.g., anxiety, afraid of being stalked, incurring financial consequences).

Citizens' concerns in relation to data donation not only focus on how their personal data is handled but the potential consequences associated with the way it is handled. This finding has implications for how smart city projects engage with citizens who are expected to donate data. It is especially important because public institutions are not the sole players in smart city projects. Partnerships with private institutions, especially those entrusted with developing the technological infrastructures on which the smart city operates are of key importance to the success of the project. These private institutions, held to the same data protection standards as public institutions, should understand the impact of the requirement for citizens to donate their personal data. Asking the citizens to participate in the design and development of smart city technologies and policies by expressing their opinions, through, for example, public consultations is an appropriate proposition to address that challenge (e.g., see

methodology employed by Ball and colleagues, 2019). MK: Smart is an example worth mentioning. MK: Smart worked closely with a community organisation (Community Action: MK) in order to understand citizens' opinions and experiences.

This thesis, in support of Nissenbaum's (2010) work, found that the risks experienced by individuals depend on their context. Accordingly, data donation requirements may impact the social fabric and how life is experienced by citizens. Certain social values may be reinforced while others discarded. Whilst for those who govern importance is generally placed on planning and efficiency of services, for citizens, it is much more than that. It means, amongst other things holding the city council accountable, be safe, and improve their commute. Smart city values quality of life, and sustainability. For this, citizens' expectations and experience should be accounted for.

Smart governments and cities developing 'smartified' environments for its citizens need to consider the implications of these findings in order to design inclusive solutions. These solutions designed by technological services providers and implemented by the local governments ought to take into account the nuances of human behaviour. Specifically, the fact that in the context of this research, privacy-specific risks alone do not construct the risks of data donation. Furthermore, the contextuality of privacy incursions, namely under what context do the risks occur should also be taken into account as well as the value privacy holds not only for people's lives, but for these individuals to exercise their self-determination that forms the basis of any democratic society.

This thesis' findings may also assist organisations developing ICTs systems in designing solutions that take into account individuals' privacy expectations together with a thorough plan of potential mitigatory actions for unwanted consequences of any privacy-specific risks. Taking this into account ensures that applications, policies, and ICTs match people's privacy expectations and the risks they may experience when deciding whether to participate in a data donation programme.

Although some may wonder “can privacy really be protected anymore?” (Ernst and Young Report, 2016)⁴⁵, this thesis responds with a resounding yes. However, one has first to abandon the idea that one-size-fits-all privacy regulations should be introduced, and that privacy is a stand-alone concern. With that approach, indeed privacy, in whatever form, may be challenging to protect.

7.8 CONCLUDING REMARKS

This thesis has drawn on two established donation and privacy risk frameworks to investigate how the risks of donating personal data to a smart city are experienced and socially constructed. The thematic analysis of the ten focus groups conducted showed that, in the context of this empirical examination, privacy-specific risks alone do not constitute constructed risks. Instead, the data demonstrated that it is the potential consequences deriving from these initially identified risks that construct the different risks of donating personal mobility data.

⁴⁵ <https://www.ey.com/gl/en/services/advisory/ey-privacy-trends-2016>

The contributions of the thesis are numerous. Alongside the empirical contribution outlined above, it has suggested a definition of data donation beyond the medical contexts in which it originally emerged. The empirical work highlights the embeddedness of privacy considerations in social interaction and the presence of privacy considerations during the act of donation, both of which can be incorporated into existing theoretical frameworks. For policy, demonstrating the social values which form the heart of privacy considerations, point to policy frameworks which need to be sensitive to those values rather than take a one-size-fits-all approach. Equally, policymakers and smart city decision-makers should consider moving beyond the focus on the issue of consent, connected with the collection of data to mobilise the rights of individuals across data processing.

With data donation set to become a routine feature of life in the Smart City, with every fabric of everyday life woven into information infrastructures, and with citizens choosing to donate their data, there are opportunities for donation, data protection and privacy to work together, constructively, to safeguard rights at these crucial developmental moments.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1), 26–33.
- Alexander, J. W., & Zola, J. C. (1996). Expanding the donor pool: use of marginal donors for solid organ transplantation. *Clinical Transplantation*, 10(1 Pt 1), 1—19. <http://europepmc.org/abstract/MED/8652891>
- Allen, A. L. (1999). Gender and privacy in cyberspace. *Stan. L. Rev.*, 52, 1175.
- Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.
- Allen, J., & Butler, D. D. (1993). Assessing the Effects of Donor Knowledge and Perceived Risk on Intentions to Donate Blood. *Journal of Health Care Marketing*, 13(3), 26–33.
<http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=9602131254&site=ehost-live>
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*.
- Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Holt, Rinehart & Winston.
- Amineh, R. J., & Asl, H. D. (2015). Review of constructivism and social constructivism. *Journal of Social Sciences, Literature and Languages*, 1(1), 9–16.
- Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4).
- Andreoni, J. (1989). Giving with Impure Altruism: Applications to Charity and Ricardian Equivalence. *Journal of Political Economy*, 97(6), 1447–1458.
<http://www.jstor.org/stable/1833247>
- Andreoni, J. (1990). Impure Altruism and Donations to Public Goods: A Theory of Warm-Glow Giving. *The Economic Journal*, 100(401), 464–477.
<https://doi.org/10.2307/2234133>

- Archea, J. (1977). The place of architectural factors in behavioral theories of privacy. *Journal of Social Issues*, 33(3), 116–137.
- Austen, L. (2009). The social construction of risk by young people. *Health, Risk & Society*, 11(5), 451–470.
- Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, 38, 33–42.
- Bailey, J., Steeves, V., Burkell, J., & Regan, P. (2013). Negotiating With Gender Stereotypes on Social Networking Sites: From “Bicycle Face” to Facebook. *Journal of Communication Inquiry*, 37(2), 91–112.
- Ball, K. (2010). Workplace surveillance: an overview. *Labor History*, 51(1), 87–106. <https://doi.org/10.1080/00236561003654776>
- Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: an empirical study. *Information Technology & People*, 25(4), 376–394.
- Ball, K., Degli Esposti, S., Dibb, S., Pavone, V., & Santiago-Gomez, E. (2018). Institutional trustworthiness and national security governance: Evidence from six European countries. *Governance*, 32(1), 103–121.
- Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body-subject. *Body & Society*, 22(2), 58–81.
- Barbour, R. (2008). *Doing focus groups*. Sage.
- Barclay, P. (2004). Trustworthiness and competitive altruism can also solve the “tragedy of the commons.” *Evolution and Human Behavior*, 25(4), 209–220. <https://doi.org/10.1016/j.evolhumbehav.2004.04.002>
- Barkhuus, L. (2012). The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 367–376.
- Barkworth, L., Hibbert, S., Horne, S., & Tagg, S. (2002). Giving at Risk? Examining Perceived Risk and Blood Donation Behaviour. *Journal of Marketing Management*, 18(9–10), 905–922. <https://doi.org/10.1362/0267257012930376>
- Barter, C., & Renold, E. (2000). “I wanna tell you a story”: exploring the application of vignettes in qualitative research with children and young people. *International Journal of Social Research Methodology*, 3(4), 307–323.
- Barter, C., & Renold, E. (1999). The use of vignettes in qualitative research. *Social Research Update*, 25(9), 1–6.

- Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. *2006 IEEE Symposium on Security and Privacy (S&P'06)*, 15-pp.
- Beauchamp, T. (2009). *Autonomy and consent. W: Miller F., Wertheimer A.(red.). The ethics of consent: theory and practice*. Oxford University Press, New York.
- Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.
- Becker, G. S. (1965). A Theory of the Allocation of Time. *The Economic Journal*, 75(299), 493. <https://doi.org/10.2307/2228949>
- Becker, M., Kolbeck, A., Matt, C., & Hess, T. (2017). Understanding the continuous use of fitness trackers: A thematic analysis. *Pacific Asia Conference on Information Systems (PACIS)*.
- Bekkers, R. (2010). Who gives what and when? A scenario study of intentions to give time and money. *Social Science Research*, 39(3), 369–381. <https://doi.org/https://doi.org/10.1016/j.ssresearch.2009.08.008>
- Benthall, S., Gürses, S., & Nissenbaum, H. (2017). *Contextual integrity through the lens of computer science*. Now Publishers.
- Benton, T., & Craib, I. (2010). *Philosophy of social science: The philosophical foundations of social thought* (2nd ed.). Oxford University Press.
- Bergstrom, T., Blume, L., & Varian, H. (1986). On the private provision of public goods. *Journal of Public Economics*, 29(1), 25–49. [https://doi.org/https://doi.org/10.1016/0047-2727\(86\)90024-1](https://doi.org/https://doi.org/10.1016/0047-2727(86)90024-1)
- Berkowitz, L. (1972). *Social Norms, Feelings, and Other Factors Affecting Helping and Altruism* (L. B. T.-A. in E. S. P. Berkowitz (ed.); Vol. 6, pp. 63–108). Academic Press. [https://doi.org/https://doi.org/10.1016/S0065-2601\(08\)60025-8](https://doi.org/https://doi.org/10.1016/S0065-2601(08)60025-8)
- Berkowitz, L., & Connor, W. H. (1966). Success, failure, and social responsibility. *Journal of Personality and Social Psychology*, 4(6), 664.
- Bishop, R. C. (2018). Warm Glow, Good Feelings, and Contingent Valuation. *Journal of Agricultural and Resource Economics*, 43(1835-2018–3853), 307–320.
- Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. *Prepared for the Annual Meeting of the American Sociological Association*, 17.
- Bradbury-Jones, C., Taylor, J., & Herber, O. R. (2014). Vignette development and administration: a framework for protecting research participants. *International*

- Journal of Social Research Methodology*, 17(4), 427–440.
<https://doi.org/10.1080/13645579.2012.750833>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Brummett, E. A., & Steuber, K. R. (2015). To reveal or conceal?: Privacy management processes among interracial romantic partners. *Western Journal of Communication*, 79(1), 22–44.
- Bryman, A., & Bell, E. (2003). *Business research methods*. (p. 778). Oxford University Press.
- Butler, P. (2020, May 1). This article is more than 7 months old UK food banks face record demand in coronavirus crisis. *The Guardian, UK*.
<https://www.theguardian.com/society/2020/may/01/uk-food-banks-face-record-demand-in-coronavirus-crisis>
- Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 6(2), 77–78.
<https://doi.org/10.1093/idpl/ipw006>
- Cardullo, P., & Kitchin, R. (2019). Being a ‘citizen’ in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. *GeoJournal*, 84(1), 1–13. <https://doi.org/10.1007/s10708-018-9845-8>
- Carsten, J. (2013). Introduction: Blood Will Out. *Blood Will Out: Essays on Liquid Transfers and Flows*, 19, 1–23. <https://doi.org/10.1002/9781118656235.fmatter>
- Carter, K. A., & Beaulieu, L. J. (1992). Conducting a community needs assessment: Primary data collection techniques. Retrieved April, 26, 2005.
- Castelnovo, W., Misuraca, G., & Savoldelli, A. (2015). Citizen’s engagement and value co-production in smart and sustainable cities. *International Conference on Public Policy*, 1–16.
- Check Hayden, E. (2013). Privacy loophole found in genetic databases. *Nature News*.
- Chiru, C. (2016). Search engines: ethical implications. *Economics, Management, and Financial Markets*, 11(1), 162–168.
- Clarke, R. (1997). *Introduction to dataveillance and information privacy and definitions of terms*. Wwww. Anu. Edu. Au/People/Roger. Clarke/DV/Intro. Html. [www. anu. edu. au/people/Roger. Clarke/DV/Intro. html](http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html)

- Clarke, R. (2006). *What's "Privacy"?* Prepared for a Workshop at the Australian Law Reform Commission on 28 July 2006.
<http://www.rogerclarke.com/DV/Privacy.html>
- Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press.
- Cooter, R., & Broughman, B. J. (2005). Charity, Publicity, and the Donation Registry. *Economists' Voice*, 2(3), 1–8. <https://doi.org/10.2202/1553-3832.1039>
- Corkery, J. M. (1992). The use of vignettes in sentencing studies of English magistrates. *International Journal of the Sociology of Law*, 20, 253.
- Crumpler, H., & Grossman, P. J. (2008). An experimental test of warm glow giving. *Journal of Public Economics*, 92(5–6), 1011–1021.
- Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Aff.*, 92, 28.
- Davis, D. D., Millner, E. L., & Reilly, R. J. (2005). Subsidy Schemes and Charitable Contributions: A Closer Look. *Experimental Economics*, 8(2), 85–106.
<https://doi.org/10.1007/s10683-005-0867-y>
- Davis, E. M. (2008). Risky business: Medical discourse, breast cancer, and narrative. *Qualitative Health Research*, 18(1), 65–76.
- Deci, E. L., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. *Journal of Research in Personality*, 19(2), 109–134. [https://doi.org/https://doi.org/10.1016/0092-6566\(85\)90023-6](https://doi.org/https://doi.org/10.1016/0092-6566(85)90023-6)
- Della Porta, D., & Keating, M. (2008). *Approaches and methodologies in the social sciences: A pluralist perspective*. Cambridge University Press.
- Department for Transport. (2018). *Walking and Cycling Statistics, England: 2017*.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/736909/walking-and-cycling-statistics-england-2017.pdf
- Dietz, T., Frey, S., & Rosa, E. (2002). Risk, technology, and society. *Handbook of Environmental Sociology*.
- Dolnicar, S., Grün, B., & Leisch, F. (2016). Increasing sample size compensates for data problems in segmentation studies. *Journal of Business Research*, 69(2), 992–999.
- Dolnicar, S., Grün, B., Leisch, F., & Schmidt, K. (2014). Required sample sizes for data-driven market segmentation analyses in tourism. *Journal of Travel Research*, 53(3), 296–306.

- Douglas, M., & Wildavsky, A. (1982). Risk and culture: An essay on the selection of environmental and technological dangers. *Berkeley: University of California Press, P12*.
- Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*(3), 319–342.
- Eckel, C. C., & Grossman, P. J. (1996). The relative price of fairness: Gender differences in a punishment game. *Journal of Economic Behavior & Organization, 30*(2), 143–158.
- Elueze, I., & Quan-Haase, A. (2018). Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin’s Privacy Attitude Typology Revisited. *American Behavioral Scientist, 62*(10), 1372–1391.
<https://doi.org/10.1177/0002764218787026>
- Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford University Press.
- Falk, A. (2007). Gift exchange in the field. *Econometrica, 75*(5), 1501–1511.
- Farnsworth, J., & Boon, B. (2010). Analysing group dynamics within the focus group. *Qualitative Research, 10*(5), 605–624.
<https://doi.org/10.1177/1468794110375223>
- Fayol, H. (1916). Teoría clásica de la Administración. *Francia*.
- FeedingAmerica. (2011). *Food Banks: Hunger’s New Staple*.
- Ferguson, E., Farrell, K., & Lawrence, C. (2008). Blood Donation is an Act of Benevolence Rather Than Altruism. *Health Psychology, 27*(3), 327–336.
<https://doi.org/10.1037/0278-6133.27.3.327>
- Finch, J. (1987). The vignette technique in survey research. *Sociology, 21*(1), 105–114.
- Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3–32). Springer.
- Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research, 20*(2), 303–315.
- Flaskerud, J. H. (1979). Use of vignettes to elicit responses toward broad concepts. *Nursing Research, 28*(4), 210–212.
- Folz, D. H. (1991). Recycling solid waste: Citizen participation in the design of a coproduced program. *State & Local Government Review, 98*–102.

- Foundation, C. A. (2019). *CAF UK Giving 2019: An overview of charitable giving in the UK*.
- Franklin, B. (1748). Advice to a young tradesman (1748). *George Fisher: The American Instructor: Or Young Man's Best Companion.... The Ninth Edition Revised and Corrected*. Philadelphia: Printed by B. Franklin and D. Hall, at the New-Printing-Office, in Market-Street, 375–377.
- Frederick, S., & Fischhoff, B. (1998). Scope insensitivity in elicited values. *Risk Decision and Policy*, 3, 109–124.
- Frey, J. H., & Fontana, A. (1991). The group interview in social research. *The Social Science Journal*, 28(2), 175–187.
- Friedman, B., Kahn Jr, P. H., Hagman, J., Severson, R. L., & Gill, B. (2006). The watcher and the watched: Social judgments about privacy in a public place. *Human-Computer Interaction*, 21(2), 235–272.
- Gaetz, S., & O'Grady, B. (2002). Making Money: Exploring the Economy of Young Homeless Workers. *Work, Employment and Society*, 16(3), 433–456.
<https://doi.org/10.1177/095001702762217425>
- Garrone, P., Melacini, M., & Perego, A. (2014). Surplus food recovery and donation in Italy: the upstream process. *British Food Journal*, 116(9), 1460–1477.
<https://doi.org/10.1108/BFJ-02-2014-0076>
- Gavison, R. (1980). Privacy and the Limits of the Law. *Yale Law Journal*, 89(3), 347.
- Gibbs, A. (2012). Focus groups and group interviews. *Research Methods and Methodologies in Education*, 186–192.
- Giddens, A. (1990). *The consequences of modernity*. John Wiley & Sons.
- Gill, P., & Lowes, L. (2008). Gift exchange and organ donation: donor and recipient experiences of live related kidney transplantation. *International Journal of Nursing Studies*, 45(11), 1607–1617.
- Gneezy, U., & Rustichini, A. (2000). Pay enough or don't pay at all. *The Quarterly Journal of Economics*, 115(3), 791–810.
- Goold, B. J. (2009). Surveillance and the Political Value of Privacy. *Amsterdam Law Forum*, 1(4), 3–6.
- Gould, D. (1996). Using vignettes to collect data for nursing research studies: how valid are the findings? *Journal of Clinical Nursing*, 5(4), 207–212.

- Grace, D., & Griffin, D. (2009). Conspicuous donation behaviour: scale development and validation. *Journal of Consumer Behaviour*, 8(1), 14–25.
<https://doi.org/10.1002/cb.270>
- Grace, D., & Griffin, D. (2006). Exploring conspicuousness in the context of donation behaviour. *International Journal of Nonprofit and Voluntary Sector Marketing*, 11(2), 147–154.
- Green, J., & Hart, L. (1999). The impact of context on data. *Developing Focus Group Research: Politics, Theory and Practice*, 21–35.
- Greene, S., & Hogan, D. (2005). Researching children's experience: Exploring children's views through focus groups. *Researching Children's Experience*. London: SAGE Publications Ltd, 237–253.
- GuardianUK. (2015). *Sharp Drop On Blood Donors*.
<https://www.theguardian.com/uk-news/2015/jun/05/sharp-drop-new-blood-donors-uk-stocks-at-risk>
- Guest, G., Namey, E., & McKenna, K. (2017). How many focus groups are enough? Building an evidence base for nonprobability sample sizes. *Field Methods*, 29(1), 3–22.
- Guterman, J. T. (2014). *Mastering the art of solution-focused counseling*. Wiley Online Library.
- Ha-Brookshire, J. E., & Hodges, N. N. (2009). Socially responsible consumer behavior?: Exploring used clothing donation behavior. *Clothing and Textiles Research Journal*, 27(3), 179–196. <https://doi.org/10.1177/0887302X08327199>
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2), 13–42.
- He, G., Boas, I., Mol, A. P. J., & Lu, Y. (2017). E-participation for environmental sustainability in transitional urban China. *Sustainability Science*, 12(2), 187–202.
- Health, U. D. of. (2016). *Body and Organ Donation in the US*.
- Hennink, M. M. (2014). *Understanding Focus Group Discussions*. Oxford University Press Oxford, UK.
- Hill, E. M. (2016). Posthumous organ donation attitudes, intentions to donate, and organ donor status: Examining the role of the big five personality dimensions and altruism. *Personality and Individual Differences*, 88, 182–186.

- Hill, M. (1997). Participatory research with children. *Child & Family Social Work*, 2(3), 171–183.
- Hoekstra, T., Twisk, D., & Hagenzieker, M. (2018). Do road user roles serve as social identities? Differences between self-described cyclists and car drivers. *Transportation Research Part F: Traffic Psychology and Behaviour*, 59, 365–377. <https://doi.org/10.1016/j.trf.2018.09.006>
- Hogg, M. A. (2000). Subjective uncertainty reduction through self-categorization: A motivational theory of social identity processes. *European Review of Social Psychology*, 11(1), 223–255.
- Holloway, I., & Todres, L. (2003). The status of method: flexibility, consistency and coherence. *Qualitative Research*, 3(3), 345–357.
- Huang, H., & Bashir, M. (2015). Direct-to-Consumer genetic testing: Contextual privacy predicament. *Proceedings of the Association for Information Science and Technology*, 52(1), 1–10.
- Hughes, R. (1998). Considering the vignette technique and its application to a study of drug injecting and HIV risk and safer behaviour. *Sociology of Health & Illness*, 20(3), 381–400.
- Hughes, R., & Huby, M. (2004). The construction and interpretation of vignettes in social research. *Social Work and Social Sciences Review*.
- Huser, V., Miller, A. W., & Vawdrey, D. K. (2014). Evaluating the size of deceased patient EHR research data sets: a multi-year trend analysis. *AMIA*.
- Isen, A. M. (1970). Success, failure, attention, and reaction to others: The warm glow of success. *Journal of Personality and Social Psychology*, 15(4), 294–301. <https://doi.org/10.1037/h0029610>
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-020-10044-1>
- Iwaarden, J. van, Wiele, T. van der, Williams, R., & Moxham, C. (2009). Charities: how important is performance to donors? *International Journal of Quality & Reliability Management*, 26(1), 5–22. <https://doi.org/10.1108/02656710910924143>
- Izuma, K., Saito, D. N., & Sadato, N. (2009). Processing of the Incentive for Social Approval in the Ventral Striatum during Charitable Donation. *Journal of Cognitive Neuroscience*, 22(4), 621–631. <https://doi.org/10.1162/jocn.2009.21228>

- Jai, T.-M. C., & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, 28, 296–303.
- Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1–2), 203–227.
- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, 47(2), 263–291.
- King, N. (2004). Using Templates in the Thematic Analysis of Text. *Essential Guide to Qualitative Methods in Organizational Research*, 256.
- Kinicki, A. J., Hom, P. W., Trost, M. R., & Wade, K. J. (1995). Effects of category prototypes on performance-rating accuracy. *Journal of Applied Psychology*, 80(3), 354–370. <https://doi.org/10.1037/0021-9010.80.3.354>
- Kitchin, R. (2015). Making sense of smart cities: addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society*, 8(1), 131–136.
- Kitkowska, A., Wästlund, E., Meyer, J., & Martucci, L. A. (2017). Is it harmful? Re-examining privacy concerns. *IFIP International Summer School on Privacy and Identity Management*, 59–75.
- Klucken, J. (2020). Does COVID change the way we DONATE our DATA? *Does COVID Change the Way We DONATE Our DATA?*
- Kourtiti, K., Deakin, M., Caragliu, A., Del Bo, C., Nijkamp, P., Lombardi, P., & Giordano, S. (2013). 11 An advanced triple helix network framework for smart cities performance. *Smart Cities: Governing, Modelling and Analysing the Transition*, 196.
- Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, 2(1), 39–63.
- Krebs, D. (1975). Empathy and altruism. In *Journal of Personality and Social Psychology* (Vol. 32, Issue 6, pp. 1134–1146). American Psychological Association. <https://doi.org/10.1037/0022-3514.32.6.1134>
- Krutzinna, J., & Floridi, L. (2019). *The ethics of medical data donation*. Springer Nature.
- Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for

- Landry, C. E., Lange, A., List, J. A., Price, M. K., & Rupp, N. G. (2006). Toward an understanding of the economics of charity: Evidence from a field experiment. *The Quarterly Journal of Economics*, 121(2), 747–782.
- Lange, A., & Stocking, A. (2009). *Charitable Memberships, Volunteering, and Discounts: Evidence from a Large-Scale Online Field Experiment*. National Bureau of Economic Research.
- Lee, J. H., Phaal, R., & Lee, S.-H. (2013). An integrated service-device-technology roadmap for smart city development. *Technological Forecasting and Social Change*, 80(2), 286–306.
- Lee, S., Ayers, S., & Holden, D. (2016). Risk perception and choice of place of birth in women with high risk pregnancies: A qualitative study. *Midwifery*, 38, 49–54.
- Leeds-Hurwitz, W. (2009). Social construction of reality. *Encyclopedia of Communication Theory*, 2, 891–894.
- Leigh, E., & Finelli, P. T. (2004). *Direct deposit donation* (Patent No. US 2005/0203837 A1). U.S. Patent Office.
- Lentine, K. L., & Patel, A. (2012). Risks and outcomes of living donation. *Advances in Chronic Kidney Disease*, 19(4), 220–228. <https://doi.org/10.1053/j.ackd.2011.09.005>
- Levine, M., Prosser, A., Evans, D., & Reicher, S. (2005). Identity and Emergency Intervention: How Social Group Membership and Inclusiveness of Group Boundaries Shape Helping Behavior. *Personality and Social Psychology Bulletin*, 31(4), 443–453. <https://doi.org/10.1177/0146167204271651>
- Levitin, A., & Redman, T. (1998). Data as a Resource: Properties, Implications, and Prescriptions. *MIT Sloan Management Review*, 40(1).
- Livingstone, S. (2005). Mediating the public/private boundary at home: children's use of the Internet for privacy and participation. *Journal of Media Practice*, 6(1).
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393–411.
- Logan, T. K., & Walker, R. (2019). The impact of stalking-related fear and gender on personal safety outcomes. *Journal of Interpersonal Violence*, 0886260519829280.
- Lohiniva, A.-L., Sane, J., Sibenberg, K., Puumalainen, T., & Salminen, M. (2020). Understanding coronavirus disease (COVID-19) risk perceptions among the

- public to enhance risk communication efforts: a practical approach for outbreaks, Finland, February 2020. *Eurosurveillance*, 25(13), 2000317.
- Lombardi, P., Giordano, S., Farouh, H., & Wael, Y. (2011). An analytic network model for Smart cities. *Proceedings of the 11th International Symposium on the AHP*, June, 15–18.
- Luhmann, N. (2002). *Risk: a sociological theory*. Routledge.
- Lyon, D. (2008). *Surveillance Society*. 1–7.
- Mantelero, A. (2014). The future of consumer data protection in the E.U. Rethinking the “notice and consent” paradigm in the new era of predictive analytics. *Computer Law and Security Review*, 2014, 643–660. <https://doi.org/10.1016/j.clsr.2014.09.004>
- Manuel, A., Solberg, S., & MacDonald, S. (2010). Organ donation experiences of family members. *Nephrol Nurs J*, 37(3), 229–236.
- Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, 59(2), 243–261.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.
- Mead, G. H. (1934). *Mind, self and society* (Vol. 111). Chicago University of Chicago Press.
- Meijer, A., & Rodríguez Bolívar, M. P. (2015). Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, 82. <https://doi.org/10.1177/0020852314564308>
- Mello, M. M., Lieou, V., & Goodman, S. N. (2018). Clinical Trial Participants’ Views of the Risks and Benefits of Data Sharing. *New England Journal of Medicine*, 378(23), 2202–2211. <https://doi.org/10.1056/NEJMsa1713258>
- Mellström, C., & Johannesson, M. (2008). Crowding out in blood donation: was Titmuss right? *Journal of the European Economic Association*, 6(4), 845–863.
- Menges, R., Schroeder, C., & Traub, S. (2005). Altruism, Warm Glow and the Willingness-to-Donate for Green Electricity: An Artefactual Field Experiment. *Environmental and Resource Economics*, 31(4), 431–458. <https://doi.org/10.1007/s10640-005-3365-y>
- Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, 59, 101151.

- Mill, J. S. (1939). Essay on liberty, 1859. In *The English Philosophers from Bacon to Mill*. Modern American Library.
- Mitchell, V. (1999). Consumer perceived risk: conceptualisations and models. *European Journal of Marketing*, 33(1/2), 163–195. <https://doi.org/10.1108/03090569910249229>
- Moorthy, J., Lahiri, R., Biswas, N., Sanyal, D., Ranjan, J., Nanath, K., & Ghosh, P. (2015). Big data: prospects and challenges. *Vikalpa*, 40(1), 74–96.
- Morgan, D. L. (1996). *Focus groups as qualitative research* (Vol. 16). Sage publications.
- Morgan, D. L. (1997). *The focus group guidebook* (Vol. 1). Sage publications.
- Morgan, S., & Miller, J. (2002). Communicating about gifts of life: the effect of knowledge, attitudes, and altruism on behavior and behavioral intentions regarding organ donation. *Journal of Applied Communication Research*, 30(2), 163–178. <https://doi.org/10.1080/00909880216580>
- Murumaa-Mengel, M., Laas-Mikko, K., & Pruulmann-Vengerfeldt, P. (2015). I have nothing to hide”: A coping strategy in a risk society. *Journalism, Representation and the Public Sphere*, 195.
- Neale, B. (1999). Post divorce childhoods. Retrieve from [Http://Www. Leeds. Ac. Uk/Family](http://www.leeds.ac.uk/Family).
- Neff, J. A. (1979). Interactional versus hypothetical others: The use of vignettes in attitude research. *Sociology and Social Research*, 64(1), 105–125.
- Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, 38, 25–36.
- Nelson, L. D., & Dynes, R. R. (1976). The Impact of Devotionalism and Attendance on Ordinary and Emergency Helping Behavior. *Journal for the Scientific Study of Religion*, 15(1), 47–59. <https://doi.org/10.2307/1384313>
- NHS. (2017). *Why Give Blood*. NHS. <https://www.blood.co.uk/why-give-blood/>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79, 119.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Nonis, S. A., Ford, C. W., Logan, L., & Hudson, G. (1996). College student’s blood donation behavior: relationship to demographics, perceived risk, and incentives. *Health Marketing Quarterly*, 13(4), 33–46.

- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1609406917733847.
- O'brien, D. M. (1979). Privacy, law, and public policy. *New York: Praeger Special Studies*.
- OpenGlasgow. (2019). *Open Glasgow: The Future of Waste and Road Repairs*.
- Patel, P. (2016). The Path to Printed Body Parts. *ACS Central Science*, 2(9), 581–583. <https://doi.org/10.1021/acscentsci.6b00269>
- Perkins, H. W. (1992). Student religiosity and social justice concerns in England and the United States: Are they still related? *Journal for the Scientific Study of Religion*, 31(3), 353–360. <https://doi.org/10.2307/1387126>
- Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.
<https://books.google.pt/books?id=gTCsft8zVXgC>
- Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, 2(3), 175–196.
- Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication*, 4(3–4), 193–207.
- Piliavin, I. M., Rodin, J., & Piliavin, J. A. (1969). Good Samaritanism: An underground phenomenon? In *Journal of Personality and Social Psychology* (Vol. 13, Issue 4, pp. 289–299). American Psychological Association.
<https://doi.org/10.1037/h0028433>
- Pilkington, H. (2007). Beyond 'peer pressure': Rethinking drug use and 'youth culture.' *International Journal of Drug Policy*, 18(3), 213–224.
- Powell, R. A., & Single, H. M. (1996). Focus groups. *International Journal for Quality in Health Care*, 8(5), 499–504.
- Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37–43.
- Raab, C. D. (2012). Privacy, social values and the public interest. *Privacy, Social Values and the Public Interest*, in A. Busch and J. Hofmann (Eds), *Politik Und Die Regulierung von Information (Politische Vierteljahresschrift, Sonderheft 46, 2012)*.

- Radin, J. M., Wineinger, N. E., Topol, E. J., & Steinhubl, S. R. (2020). Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study. *The Lancet Digital Health*, 2(2), e85–e93. [https://doi.org/10.1016/S2589-7500\(19\)30222-5](https://doi.org/10.1016/S2589-7500(19)30222-5)
- Rawlings, E. I. (1970). Reactive guilt and anticipatory guilt in altruistic behavior. *Altruism and Helping Behavior*, 163–177.
- Redcross. (2018). *Redcross' way of donating*. Making a Donation. <http://www.redcross.org.uk/Donate-Now/Donation-enquiries/Making-a-donation>
- Regan, P. M. (1995). Legislating Privacy: Technology. *Social Values, and Public Policy*, 69.
- Regan, P. M. (2015). Privacy and the common good: revisited. *Social Dimensions of Privacy: Interdisciplinary Perspectives*, 50.
- Regan, P. M., & Steeves, V. (2010). Kids r us: online social networking and the potential for empowerment. *Surveillance & Society*, 8(2), 151–165.
- Regnerus, M. D., Smith, C., & Sikkink, D. (1998). Who Gives to the Poor? The Influence of Religious Tradition and Political Location on the Personal Generosity of Americans toward the Poor. *Journal for the Scientific Study of Religion*, 37(3), 481–493. <https://doi.org/10.2307/1388055>
- Reicher, S., Spears, R., & Haslam, S. A. (2010). *The SAGE Handbook of Identities*. SAGE Publications Ltd. <https://doi.org/10.4135/9781446200889>
- Reinsel, D., Gantz, J., & Rydning, J. (2017). Data Age 2025: The Evolution of Data to Life-Critical. In *IDC White Paper; Sponsored by Seagate* (Issue April). <http://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>
- Roberts, R. D. (1984). A Positive Model of Private Charity and Public Transfers. *Journal of Political Economy*, 92(1), 136–148. <http://www.jstor.org/stable/1830550>
- Rodriguez, K., & Windwehr, S. (2020). *Workplace Surveillance in Times of Corona*. <https://www.eff.org/deeplinks/2020/09/workplace-surveillance-times-corona>
- Rogers, Z. F. (2014). *Wearing your heart on your sleeve: The effects of conspicuous compassion on identity signaling and charitable behavior*. City University of New York.
- Rule, J. B. (2019). Contextual Integrity and its Discontents: A Critique of Helen Nissenbaum's Normative Arguments. *Policy & Internet*, 11(3), 260–279. <https://doi.org/https://doi.org/10.1002/poi3.215>

- Russell, L. D., & Babrow, A. S. (2011). Risk in the making: Narrative, problematic integration, and the social construction of risk. *Communication Theory*, 21(3), 239–260.
- Russell, S., & Jacob, R. G. (1993). Living-related organ donation: The donor's dilemma. *Patient Education and Counseling*, 21(1), 89–99. [https://doi.org/10.1016/0738-3991\(93\)90063-3](https://doi.org/10.1016/0738-3991(93)90063-3)
- Ryan, G. W., & Bernard, H. R. (2000). *Data management and analysis methods*.
- Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., Detmer, D. E., & Panel, E. (2007). Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association : JAMIA*, 14(1), 1–9. <https://doi.org/10.1197/jamia.M2273>
- Sayre, S., & Horne, D. (2000). Trading secrets for savings: How concerned are consumers about club cards as a privacy threat? *ACR North American Advances*.
- Schneider, F. (2013). The evolution of food donation with respect to waste prevention. *Waste Management*, 33(3), 755–763.
- Scholl, H. J., & Scholl, M. C. (2014). Smart governance: A roadmap for research and practice. *IConference 2014 Proceedings*.
- Shaw, G. B. (1896). SOCIALISM FOR MILLIONAIRES. *The Contemporary Review, 1866-1900*, 69, 204–217.
- Shaw, R. M. (2019). Altruism, solidarity and affect in live kidney donation and breastmilk sharing. *Sociology of Health & Illness*, 41(3), 553–566.
- Sheppard, M., & Ryan, K. (2003). Practitioners as rule using analysts: A further development of process knowledge in social work. *British Journal of Social Work*, 33(2), 157–176.
- Siddiqui, S., & Tee, L. H. (2019). What Intensivists Say About an Opt-Out System for Organ Donation. *Transplantation Proceedings*, 51(6), 1651–1654.
- Sim, J., & Waterfield, J. (2019). Focus group methodology: some ethical challenges. *Quality & Quantity*, 53(6), 3003–3022.
- Skatova, A., & Goulding, J. (2019). Psychology of personal data donation. *PLOS ONE*, 14(11), e0224240. <https://doi.org/10.1371/journal.pone.0224240>
- Skatova, A., Ng, E., & Goulding, J. (2014). Data Donation: Sharing Personal Data for Public Good. *Application of Digital Innovation. London, England: N-Lab*.

- Smith, A., Matthews, R., & Fiddler, J. (2013). Recruitment and retention of blood donors in four Canadian cities: an analysis of the role of community and social networks. *Transfusion*, 53, 180S-184S.
- Sokal, A. D. (1996). Transgressing the boundaries: Toward a transformative hermeneutics of quantum gravity. *Social Text*, 46/47, 217–252.
- Solove, D. (2008). *Understanding privacy*.
- Solove, D. J. (2006). A taxonomy of privacy. *U. Pa. L. Rev.*, 154(3), 477.
- Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44, 745.
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- Solove, D. J. (2015). The meaning and value of privacy. *Social Dimensions of Privacy: Interdisciplinary Perspectives*, 71.
- Sosenko, P. (2019). *The State of Hunger: A study of poverty and food insecurity in the UK*.
- Spector, M., & Kitsuse, J. I. (2001). *Constructing Social Problems*. New Brunswick. *Transactions Publisher*.
- Steeves, V. (2015). Privacy, sociality and the failure of regulation: Lessons learned from young Canadians' online experiences. *Social Dimensions of Privacy: Interdisciplinary Perspectives*, 244–260.
- Steeves, V. (2009). Reclaiming the social value of privacy. *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, 191–208.
- Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: do cognitive heuristics hold the key? *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 811–816.
- Sundeen, R. A., Raskoff, S. A., & Garcia, M. C. (2007). Differences in perceived barriers to volunteering to formal organizations: Lack of time versus lack of interest. *Nonprofit Management and Leadership*, 17(3), 279–300.
<https://doi.org/10.1002/nml.150>
- Talbot, D. (2008). How Obama Really Did It. *Technology Review by MIT*, 9.
<https://www.technologyreview.com/s/410644/how-obama-really-did-it/>
- Tao, Z. (2017). Understanding location-based services users' privacy concern: An elaboration likelihood model perspective. *Internet Research*, 27(3), 506–519.
<https://doi.org/10.1108/IntR-04-2016-0088>

- Taylor, D. A. (1968). The development of interpersonal relationships: Social penetration processes. *The Journal of Social Psychology*, 75(1), 79–90.
- Taylor, D. A., & Altman, I. (1975). Self-disclosure as a function of reward-cost outcomes. *Sociometry*, 18–31.
- Taylor, F. W. (1911). The principles of scientific management. *New York*, 202.
- TheSun. (2017). *Donor Need: The Sun*.
<https://www.thesun.co.uk/fabulous/3626923/give-blood-donate-day/>
- Thompson, J., Petronio, S., & Braithwaite, D. O. (2012). An examination of privacy rules for academic advisors and college student-athletes: A communication privacy management perspective. *Communication Studies*, 63(1), 54–76.
- Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: a meta-analysis. *Computers in Human Behavior*, 93, 1–12.
- Titmuss, R. M. (1970). The gift relationship. From human blood to social policy. In *The gift relationship. From human blood to social policy*. London: George Allen & Unwin Ltd.
- Tonin, M., & Vlassopoulos, M. (2014). An experimental investigation of intrinsic motivations for giving. *Theory and Decision*, 76(1), 47–67.
<https://doi.org/10.1007/s11238-013-9360-9>
- Tonin, M., & Vlassopoulos, M. (2013). Experimental evidence of self-image concerns as motivation for giving. *Journal of Economic Behavior & Organization*, 90, 19–27.
- Transplant, N. H. S. B. and. (2020). *National Health Service Blood and Transplant*.
<https://www.nhsbt.nhs.uk/>
- Tuckett, A. G. (2005). Applying thematic analysis theory to practice: A researcher's experience. *Contemporary Nurse*, 19(1–2), 75–87.
- Tyler, G. (2020). *Food Banks in the UK*.
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) (testimony of European Union). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>
- Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472–480.

- Veblen, T. (1912). *The theory of the leisure class*. Routledge.
- Verpy, H., Smith, C., & Reicks, M. (2003). Attitudes and Behaviors of Food Donors and Perceived Needs and Wants of Food Shelf Clients. *Journal of Nutrition Education and Behavior*, 35(1), 6–15.
[https://doi.org/https://doi.org/10.1016/S1499-4046\(06\)60321-7](https://doi.org/https://doi.org/10.1016/S1499-4046(06)60321-7)
- Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication*, 17(1), 101–115.
- Watson, T. J. (1994). Managing, crafting and researching: words, skill and imagination in shaping management research. *British Journal of Management*, 5, S77–S87.
- Weber, M. (1947). *Max Weber, the theory of social and economic organization*. New York : Free Press ; London : Collier Macmillan, [1947] ©1947.
<https://search.library.wisc.edu/catalog/999697724602121>
- Webster, C. W. R., & Leleux, C. (2018). Smart governance: Opportunities for technologically-mediated citizen co-production. *Information Polity*, 23(1), 95–110.
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, 16(4), 409–421.
<https://doi.org/10.1287/orsc.1050.0133>
- Weisman, J., & Brosgole, L. (1994). Facial affect recognition in singly diagnosed mentally retarded people and normal young children: a methodological comparison. *International Journal of Neuroscience*, 75(1–2), 45–55.
- West, P. (2004). *Conspicuous compassion: Why sometimes it really is cruel to be kind*. Civitas/Inst for the Study of.
- Westin, A. F. (2000). Intrusions. *Public Perspective*, 11(6), 8–11.
- Westin, A. F., & Ruebhausen, O. M. (1967). *Privacy and freedom* (Vol. 1). Atheneum New York.
- WHO. (2018). *Blood Safety - Data And Statistics*.
<http://www.euro.who.int/en/health-topics/Health-systems/blood-safety/data-and-statistics>
- Wood, D. M., & Mackinnon, D. (2019). Partial platforms and oligoptic surveillance in the smart city. *Surveillance & Society*, 17(1/2), 176–182.

- Woodruff, A., Pihur, V., Consolvo, S., Brandimarte, L., & Acquisti, A. (2014). Would a Privacy Fundamentalist Sell Their {DNA} for \$1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 1–18.
- WRAP. (2020). *Food waste falls by 7% per person in three years*.
- Young, E. and. (2016). *Can Privacy Still Be Protected?*
- Zabihzadeh, A., Mazaheri, M. A., Hatami, J., Nikfarjam, M. R., Panaghi, L., & Davoodi, T. (2019). Cultural differences in conceptual representation of “Privacy”: A comparison between Iran and the United States. *The Journal of Social Psychology*, 159(4), 357–370.
- Zizzo, D. J. (2010). Experimenter demand effects in economic experiments. *Experimental Economics*, 13(1), 75–98. <https://doi.org/10.1007/s10683-009-9230-z>

APPENDICES

APPENDIX 1 – KEY INFORMANT INTERVIEWS

QUESTIONNAIRE

Semi-Structured Key Informant Interview (These were the topics guiding the interviews. Some topics were flowing from the conversation, while others had to be asked directly).

1 – Introductions

2 – Introduce the research and explain the premise behind data donation

3 – What are the different ways MK: Smart collects citizens' data (especially focused on mobility data)?

4 – How is the data being mined and actionable insights generated?

5 – Are citizens aware that their data is being collected? How does MK: Smart seek consent?

6 – Are there any acknowledged risks while collecting and using people's personal data?

7 – Under the definition of data donation I previously suggested, is MK: Smart asking citizens to donate personal mobility data?

8 – What is the purpose and how is the data used for the benefit of the citizens?

9 – How are citizens recruited to participate in the project?

10 – What are the main advantages of having people donating their data to a smart city, instead of just collecting it through, for example, sensors?

11 – What advantages do you see smart cities bringing to their citizens' daily lives? What about disadvantages?

12 – (only to one of the participants) You recently authored an article where you claimed that 'public participation can be seen as a solution for surveillance and privacy concerns'. What surveillance and privacy concerns are the most expressed by Milton Keynes' citizens and how does MK: Smart work to mitigate them?

13 – Thank you very much for participating. (Chance for a Q&A with the interviewer).

APPENDIX 2 – FOCUS GROUPS RECRUITMENT

QUESTIONNAIRE

Recruitment Questionnaire employed by QRS (Agency tasked with recruiting the participants).

Name of Participant	
Address (inc. postcode)	
Tel No. (inc. STD code)	

IMPORTANT

Please indicate with a ✓ below the method of recruitment used for this participant:

Telephone	1
Data base	2
In street, face to face	3
From client lists	4

IF YOU ARE USING DATABASE PLEASE ONLY PROCEED ONCE YOU'VE SPOKEN TO THE QRS PROJECT MANAGER. YOU MAY ONLY USE A DATABASE IF YOU HAVE PASSED THE GDPR AUDIT AND THE IT SECURITY QUESTIONNAIRE.

IF DATABASE

When was consent obtained for the participant to join your database?

Please provide a copy of the consent wording to QRS.

PLEASE NOTE:

You must NOT knowingly recruit friends/relatives to the same group/depths or another group/depths on the same project.

Fully completed questionnaires must be returned to QRS office with your payclaim as soon as the groups have taken place.

Any storage of participants data or confidential information on this project must be undertaken in accordance with the QRS Data Protection and IT Security Policy. Please indicate here that you have read our policies and agree to adhere to them.

I agree YES (please circle)

Good morning/afternoon. My name is...	
I am working on behalf of QRS Research an independent market research company who are currently conducting a research project about....	How individuals construct the risks of donating their personal mobility data to a smart city project.
The research for this project is being conducted on behalf of....	St Andrews University
and their client is...	Will be confirmed at the group
The purpose is of research	This project aims to understand how individuals construct the risks of donating their personal mobility data to a smart city project. You do not need to have any technical, or specific, knowledge to participate in this research. Instead, I am interested in exploring your opinions, beliefs, and attitudes regarding this topic. Furthermore, it is important that you are aware that the conversation will be informal and will evolve around a number of fictional scenarios, and there are no right or wrong answers.

This project is purely for market research purposes only and is being conducted in accordance with Market Research Society Code of Conduct. We will ensure that you will remain anonymous and your details kept confidential at all times unless you have given your permission otherwise.

You have the right to withdraw consent at any stage and have the right to access data collected about you. We may use your contact details for the purposes of validation and quality control. Any further contact after the research project would only be undertaken if you have given your consent for us to do so.

The market research session maybe audio and video-recorded and photos may be taken. Your name and some of your contact details will be kept on record to show your participation. This information is for market research purposes & will be kept confidential. Please be assured that these recordings are only ever used for the purposes of analysis and presentation of the findings.

It will not be used to identify you or be transferred to any third party without your consent & is held in line with Data Protection.

This questionnaire will take no longer than	10 mins to complete <i>(This will be dependent on your responses)</i>	
And will determine if you are eligible to take part in a	Depth 1	Acc Shop 3
	Group 2	Other 4
The duration of this session will be	1 hour	
The research will take place at	Meeting Room 10, 2 nd floor, Jennie Lee Building, The Open University, Walton Hall MK7 6AA, United Kingdom	
You will receive an incentive of This is to cover any out of pocket expenses	£40	
The incentive will be paid by	QRS 1	Research Client 2

As part of this project, we will be collecting data on

1	Gender	6	Marital status
2	Age	7	Working status
3	Cycling habits	8	Lifestage
4	Religion	9	Medical information
5	Political views	10	

The reason we ask for this data is so that we can speak to **a wide range of people and ensure representativeness and speak to the people that our client is most interested in for this study.**

Based on the information given to you, if you're happy to proceed then I need to ask you a series of questions in order to ascertain whether you are eligible to participate in this research...

I agree to participate in the survey and provide the personal sensitive data that I have been notified of for research purposes	Yes	No
--	-----	----

Great, before we can confirm your participation, I need to ask you a few questions to ensure the study is relevant for you.

QA	<i>Firstly then, could you please tell me if you live in, or commute to, Milton Keynes?</i>	
1	Yes	CONTINUE
2	No	CLOSE

ONLY RECRUIT THOSE WHO LIVE IN, OR COMMUTE TO, MILTON KEYNES

QB	<i>Have you ever taken part in a market research discussion or interview before?</i>	
1	Yes	CONTINUE
2	No	CONTINUE GO TO QF

QC	<i>How many times have you attended a group discussion or been interviewed?</i>	
1	Once	CONTINUE
2	2-3 times	CONTINUE
3	More than 3 times	CLOSE

IF PARTICIPANT HAS EVER ATTENDED MORE THAN 3 GROUPS OR INTERVIEWS, THEN PLEASE CLOSE

QD	<i>And when was the last time you attended a market research group or interview?</i>	
1	In the last 6 months	CLOSE
2	More than 6 months ago	CONTINUE

IF PARTICIPANT HAS ATTEND A GROUP DISCUSSION OR INTERVIEW IN THE LAST 6 MONTHS, THEN PLEASE CLOSE

QE	<i>What was the subject of the group discussions/interviews you attended?</i>	
Write in		

IF ON A SIMILAR SUBJECT THEN PLEASE DO NOT RECRUIT

QF	<i>Gender</i>	
	I identify my gender as	write in

GROUPS – 1, 4, 5, 8, 9, 12 TO BE MALES ONLY
GROUPS – 2, 3, 6, 7, 10, 11 TO BE FEMALES ONLY
GROUPS 13 & 14 TO BE HALF MALE AND HALF FEMALES IN EACH GROUP

PLEASE BE AWARE THAT ALMOST ALL THE FOCUS GROUPS ARE GENDER SPECIFIC. THEREFORE, WHEN PROVIDING THE DATE AND TIME OPTIONS, BE MINDFUL TO PROVIDE ONLY THE SUITABLE SCHEDULING OPTIONS]
[EACH GROUP SHOULD HAVE 6 X PARTICIPANTS]
[MIXED GROUPS SHOULD HAVE AN APPROXIMATE EQUAL NUMBER OF BOTH MALE AND FEMALE PARTICIPANTS - IDEALLY 3 X MALES AND 3 X FEMALES]

QG	<i>May I just ask which of the following age categories you fall into?</i>	
1	18 -34 yrs	CLOSE
2	35-39 yrs	CONTINUE
3	40-49 yrs	CONTINUE
4	50-59 yrs	CLOSE
5	60 or older	CLOSE

ONLY INDIVIDUALS AGED BETWEEN 35 TO 49 SHOULD BE RECRUITED

QH	<i>Please can you tell me how often do you cycle (per week)?</i>	
1	Never	CLOSE
2	Once or Twice	CONTINUE
3	More than Twice but not every day	CONTINUE
4	Every day	CONTINUE

ONLY INDIVIDUALS WHO CYCLE AT LEAST ONCE PER WEEK SHOULD BE RECRUITED

QI Please can you tell me, what is your average bicycle journey time?

QJ In which country were you born and how long have you lived in the UK?

WRITE IN COUNTRY OF BIRTH _____

LENGTH OF TIME LIVED IN THE UK _____

ALL RESPONDENTS MUST HAVE LIVED IN THE UK FOR AT LEAST 10 YEARS

QK I'm now going to ask you a slightly different question!

QH I'm going to read a list of statements that may or may not describe you personally. I want you _____ to rate the degree to which the statement describes you on a scale of 1 to 10, where 10 describes _____ you completely and 1 does not describe you at all.		
		Score 1-10
A	<i>If asked to describe something, I can usually do so in detail</i>	
B	I get excited about doing something I have not done before	
C	<i>My friends consider me friendly and outgoing</i>	
D	I look at and even enjoy some advertising	
E	I like to use my imagination to come up with new ideas	
F	<i>I am open about expressing my thought and feelings</i>	
G	<i>I enjoy meeting and talking to new people</i>	
H	<i>I am comfortable talking with others even if I haven't met them before</i>	
I	I see myself as creative	
J	<i>I enjoy interacting with others in group discussions and am open to hearing other people's thoughts, ideas and opinions</i>	

ALL RESPONDENTS MUST CODE AT LEAST 7 OR MORE FOR STATEMENTS
A, C, F, G, H and J

CONSENT FOR RECORDING AND/OR VIEWING

Q1 This session will be audio recorded do you give your consent for this?		
1	Yes	
2	No	

Q2 There may be clients observing these sessions do you give your consent for this?		
1	Yes	
2	No	

THE RECORDINGS TAKEN WILL ONLY BE USED FOR MARKET RESEARCH PURPOSES/ANALYSIS AND PRESENTATION OF THE FINDINGS. AT NO TIME WILL YOUR DETAILS BE PASSED ONTO ANYONE NOT CONNECTED TO THIS RESEARCH PROJECT

RE-CONTACT

Q3 If QRS or our client needed to contact you again specifically regarding this research study do you give your consent for us to do so?		
1	Yes	
2	No	

PLEASE ASK THIS QUESTION TO ENSURE THAT WE ARE ADHERING TO THE DATA PROTECTION ACT IN THE EVENT OF NEEDING TO RE-CONTACT THE PARTICIPANT AGAIN FOR MARKET RESEARCH

Q4	<i>You may be contacted by us for validation purposes do you give consent for this?</i>	
1	Yes	CONTINUE
2	No	CLOSE

Q5	<i>We will store your information including contact details for 24 months for quality control purposes</i> <i>After 24 months the information that you have given us will be securely destroyed.</i> <i>Do you give your consent for this?</i>	
1	Yes	
2	No	

Q6	<i>You will be asked to present proof of identification upon arrival to the venue. Are you happy to do this?</i>	
1	Yes	
2	No	

Q7	<i>You will be asked to sign a consent form on the day will this be OK?</i>	
1	Yes	
2	No	

Q8	<i>Finally, further details on our privacy policy can be viewed at</i> http://www.qrs-research.co.uk/privacy-policy https://www.st-andrews.ac.uk/development/your-data-and-privacy/ https://www.st-andrews.ac.uk/assets/university/data-protection/gdpr-dpr-research-guidance.pdf <i>I must just express to you that by participating in this research anything disclosed during the course of the discussion should not be discussed with anyone outside of the discussion environment. Likewise anything you say will remain confidential and non attributable. You may be asked to sign a Non-disclosure agreement prior to being included in the discussion.</i>	
1	Yes I accept this	CONTINUE
2	No I don't accept this	CLOSE

- **IF RESPONDENTS HAVE A MOBILE PHONE WITH THEM, IT MUST BE SWITCHED OFF (NOT JUST ON SILENT) DURING THE INTERVIEW.**
- **IF RESPONDENTS REQUIRE SPECTACLES TO READ THEY MUST BRING THEM TO THE INTERVIEW.**

Please choose the date and time that better suits you:

Monday 16th September – 6 PM	1	MALE
Monday 16 th September – 7 PM	2	FEMALE
Tuesday 17 th September – 6 PM	3	FEMALE
Tuesday 17 th September – 7 PM	4	MALE
Wednesday 18 th September – 6 PM	5	MALE
Wednesday 18 th September – 7 PM	6	FEMALE
Thursday 19 th September – 6 PM	7	FEMALE
Thursday 19 th September – 7 PM	8	MALE
Friday 20 th September – 6 PM	9	MALE
Friday 20 th September – 7 PM	10	FEMALE
Saturday 21 st September – 10 AM	11	FEMALE
Saturday 21 st September – 11 AM	12	MALE
Sunday 22 nd September – 10 AM	13	MIXED
Sunday 22 nd September – 11 AM	14	MIXED

**[PLEASE BE AWARE THAT ALMOST ALL THE FOCUS GROUPS ARE GENDER SPECIFIC. THEREFORE, WHEN PROVIDING THE DATE AND TIME OPTIONS, BE MINDFUL TO PROVIDE ONLY THE SUITABLE SCHEDULING OPTIONS]
[EACH GROUP SHOULD HAVE BETWEEN 6 AND 10 PARTICIPANTS]
[MIXED GROUPS SHOULD HAVE AN APPROXIMATE EQUAL NUMBER OF BOTH MALE AND FEMALE PARTICIPANTS]**

Thank you very much for providing the time that better suits you.

UPON RESPONDENTS AGREEMENT OF ATTENDANCE: PLEASE confirm date of attendance and confirm meeting address – hand letter of invitation.

RECRUITERS DECLARATION

I (name of recruiter) herewith declare that the participant has given me all answers of his/her own free will; I have not influenced the participant in any of his/her answers. I have carried out the interview solely in accordance with the regulations and instructions. All statements reflect the truth.

I have carried out the interview in accordance with the above-mentioned instructions and in accordance with the British Market Research Society Code of Conduct to the best of my ability.

The participant has declared himself/herself willing to take part in the group discussion of his/her own accord.

Furthermore, the participant has been informed that the session will be recorded for research purposes. The participant has been informed that the client may possibly view the recording – in accordance with MRS code of conduct. The participant has been assured that the recording will be anonymous (no name, address or other such information). The participant agrees to take part in the discussion under these terms. I also confirm that I have provided the recruited participant with the QRS letter of invitation and provided the explanation about incentive payments.

I hereby confirm that all above-mentioned information has been passed on to the participant and that the participant has agreed to all points.

<i>SIGNED :</i>	
<i>DATE :</i>	
<i>PRINTED NAME :</i>	

APPENDIX 3 - VIGNETTES

VIGNETTES:

BACKGROUND INFORMATION:

Kris is 43-year-old and works as a bank clerk in Mossford Council. Kris lives 40 minutes away from work and commutes every day by bicycle.

1st Vignette:

Kris is asked by Mossford City Council to participate in their Active Travel Programme, part of their wider Smart City project. In order to participate, all Kris has to do is to install an application on a smartphone that will track location, elevation, routes taken, speed, among other things.

Also, Kris can video-record and take pictures to road dangers, such as potholes and dangerous intersections, and comment in the app how easy certain portions of the route are.

Q – Do you think Kris will agree to participate in this project? Please explain why.

2nd Vignette:

Kris has not yet decided what to do. On one hand, it is believed that this is a great way to show others where potholes are, how dangerous a certain intersection is, and whether or not the route Kris takes is easy for beginners. It is also a way of holding the city council accountable for the conditions of the road.

On the other hand, Kris believes that, sometimes, stopping to record these issues may be time-consuming, especially if Kris is late to work.

Q – Do you think Kris will agree to participate in this project? Please explain why.

3rd Vignette:

Kris has now been informed that the council will provide a watch that tracks the heart rate. Besides tracking the heart rate, Kris was also asked to provide weight data to the application on a regular basis. The council argues that this data is needed to study physical effort levels while cycling in different parts of the city.

Q – Do you think Kris will agree to participate in this project? Please explain why.

4th Vignette:

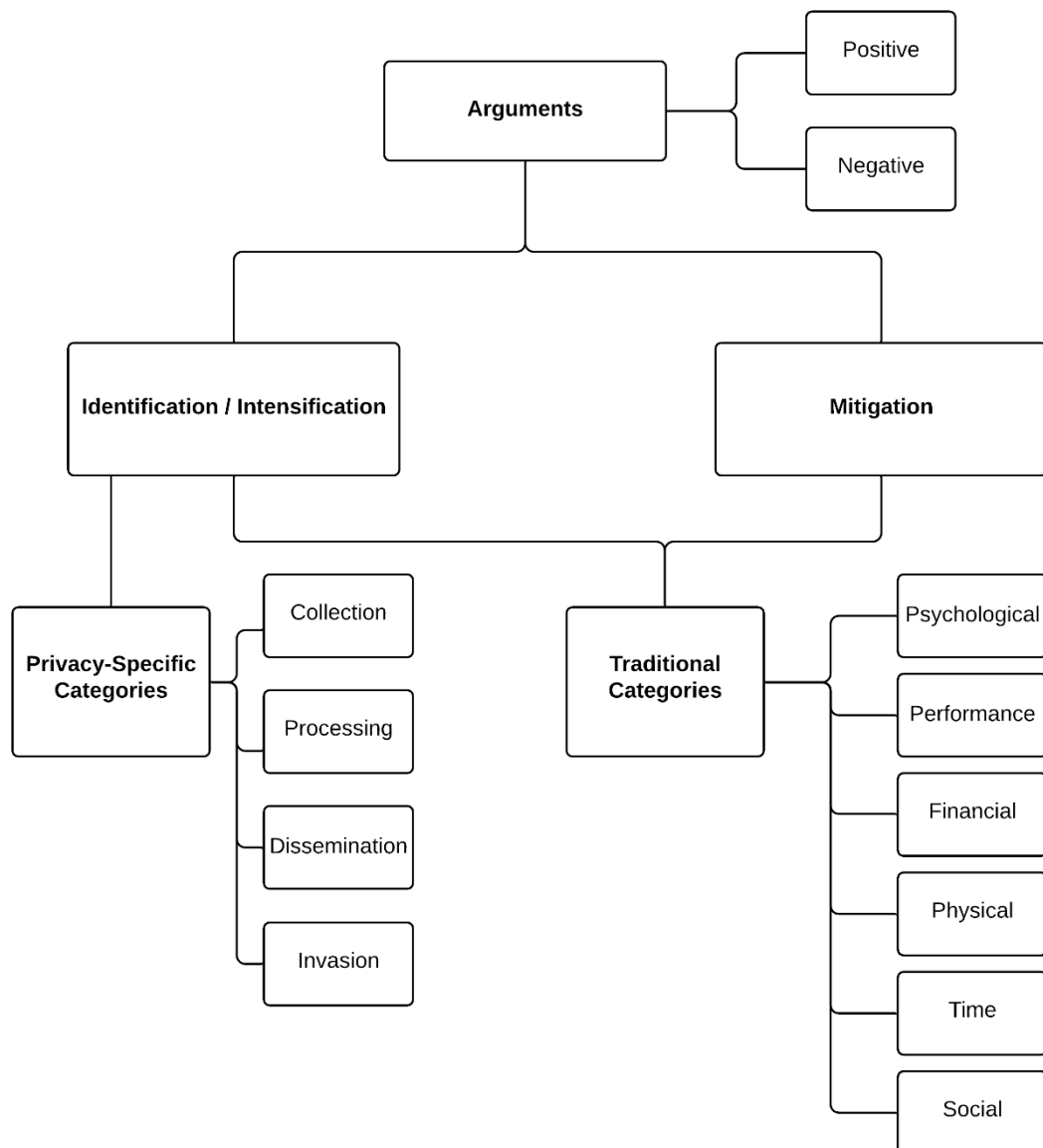
Kris has been using the app for 6 months.

Yesterday Kris received a letter from the car insurance company informing that the annual premium has increased by 35%. Kris has been informed that erratic driving behaviour led to an increase in the premium.

The city council disclosed Kris' data to the insurer without asking for Kris' consent.

Q – Do you think Kris will continue to participate in this project? Please explain why.

APPENDIX 4 – CODING TREE



APPENDIX 5 – ETHICS AUTHORISATION



University Teaching and Research Ethics Committee

02 July 2019

Dear Jorge

Thank you for submitting your ethical application which was considered by the School of Management Ethics Committee on 1st July 2019 when the following documents were reviewed:

1. Ethical Application Form
2. Participant Information Sheet
3. Consent Form
4. Debriefing Form

The School of Management Ethics Committee has been delegated to act on behalf of the University Teaching and Research Ethics Committee (UTREC) and has granted this application ethical approval. The particulars relating to the approved project are as follows -

Approval Code:	MN14450	Approved on:	1/7/19	Approval Expiry:	1/7/24
Project Title:	Risk Perceptions in the Donation of Mobility Data				
Researcher(s):	Jorge Fernando Pereira Campos				
Supervisor(s):	Kirstie Ball				

Approval is awarded for five years. Projects which have not commenced within two years of approval must be re-submitted for review by your School Ethics Committee. If you are unable to complete your research within the five year approval period, you are required to write to your School Ethics Committee Convener to request a discretionary extension of no greater than 6 months or to re-apply if directed to do so, and you should inform your School Ethics Committee when your project reaches completion.

If you make any changes to the project outlined in your approved ethical application form, you should inform your supervisor and seek advice on the ethical implications of those changes from the School Ethics Convener who may advise you to complete and submit an ethical amendment form for review.

Any adverse incident which occurs during the course of conducting your research must be reported immediately to the School Ethics Committee who will advise you on the appropriate action to be taken.

Approval is given on the understanding that you conduct your research as outlined in your application and in compliance with UTREC Guidelines and Policies (<http://www.st-andrews.ac.uk/utrec/guidelinespolicies/>). You are also advised to ensure that you procure and handle your research data within the provisions of the Data Provision Act 1998 and in accordance with any conditions of funding incumbent upon you.

Yours sincerely

Convener of the School Ethics Committee

cc Supervisor

School of Management Ethics Committee, The Gateway, North Haugh, St Andrews, Fife, KY16 9SS
management.ethics@st-andrews.ac.uk

The University of St Andrews is a charity registered in Scotland: No SC013532

APPENDIX 6 – ETHICS APPLICATION FORM



University of
St Andrews

University Teaching and Research Ethics Committee (UTREC) Application Form

Please ensure that you have included all of the relevant documents in your application.

If all relevant documents are not included, your application will be returned without review

Ethical Application Form	YES
Participant Information Sheet	YES
Participant Consent Form	YES
Participant Debriefing Form	YES
Data Management Plan Do you already have a data management plan (DMP) at the point of starting to complete this form? If YES, when you submit this form, please append the DMP, and also email a copy to research-data@st-andrews.ac.uk . If NO, please ignore this question.	Click to select
All advertisements (online/paper)	Click to select
Copies of Questionnaire / Online Survey Screenshots	YES
Semi/Structured interview questions/Focus Group guide	YES
External permission forms / emails	YES
NHS ethical approval documents in full	Click to select
DBS / PVG documents	Click to select
Copies of letters to parents/guardians/children	Click to select
Fieldwork risk assessment form (where appropriate)*	Click to select
Sensitive research declaration	Click to select
Ethical funder approval	Click to select

If ethical approval has been obtained from the University of St Andrews for research so similar to this project that a new review process may not be required, please give details of the application and the date of its approval.

Approval Code:	
Date Approved:	Click or tap to enter a date.
Project Title:	
Researchers Name(s):	

(* Please note that a signed hard-copy of the fieldwork risk assessment form is required, in addition to the electronic copy, where appropriate)

Please list below any other documents that are included in your application:

Signature			
Applicant (staff/student)	Student	Date	06/06/2019
Print name	Jorge Campos		

Researcher Name	Jorge Fernando Pereira Campos
------------------------	-------------------------------

Undergraduate	<input type="checkbox"/>	Staff	<input type="checkbox"/>
Postgraduate Research	<input checked="" type="checkbox"/>	Postgraduate Taught	<input type="checkbox"/>
Module Co-ordinator on taught module	<input type="checkbox"/>	Module Code	

Project Title:	Risk Perceptions in the Donation of Mobility Data		
School/Unit:	Management	Supervisor:	Kirstie Ball / Sally Dibb
Email	jfpc@st-andrews.ac.uk	Date Submitted	06/06/2019

Project description: Please give a concise description without technical terminology of **what** you are proposing to do; **Who** your participants are (eg. age, vulnerability, nationality, organisation); **Where** the research will take place (eg. site, country); **How** you are doing it, (eg. survey, interview). *(900 characters for database reasons)*

This project aims to understand how individuals perceive the risks involved in donating their personal mobility data to a smart city project. In order to explore this phenomenon, it is necessary to conduct scenario-based focus groups so that discursive patterns related to the construction of risk can be elicited. Seven sets of focus groups, each set comprising two focus groups, will be run in Milton Keynes (locations are being investigated). The participants are people aged 35 to 49, who live in, or commute to Milton Keynes. Additionally, in order to exclude views of other individuals who do not use a smartphone and cycle, and, that in consequence, might have different discourses, it is crucial to recruit participants who cycle, for commute or pleasure purposes, and own, and use, a smartphone.

Ethical Considerations: You should give an overview of the important ethical issues raised by your research including **how** you will obtain voluntary informed consent (especially where you are gathering audio/video data); **What** type of data you will be collecting (anonymous, pseudonymised, identifiable); **How** you will handle, store and retain/destroy data. *(900 characters for database reasons)*

Data will be gathered by recording the audio of the focus group conversation directly to an encrypted and backed-up external hard drive. Data collected will be qualitative and non-attributable. However, to enable participants to register in the focus group, some personal data will inevitably be collected, such as name, surname, and city of residence. This data, however, will be kept separate from the transcribed data. Any collected data will be stored in an encrypted and backed-up external hard drive only accessible by the researcher and supervisors, and, three years after the research project is finished, the data will be completely destroyed. Additionally, focus groups data will be transcribed by a third-party company, according to a template I have created. Informed consent will be requested by me before the start of data collection. Therefore, before the start of the focus group, I will ask the participants to sign the relevant consent forms.

RESEARCH INFORMATION		
1. Estimated start date	16/09/2019	
2. Estimated duration of	Data collection will take a maximum of two weeks	
3. a.	Is this research funded by any external sponsor or agency?	YES
	<p>If YES, please provide the name of the funder:</p> <p>The participant recruitment is being funded by the 'Big Data Surveillance' partnership grant.</p> <p>The grant is funded by the Social Sciences and Humanities Research Council of Canada reference SSHRC 895-2015-1003</p>	
b.	Does the funder appear on the automatically approved list of ethical funders?	YES
<p>You should ensure that you are familiar with the conditions of funding incumbent upon you. In particular there may be a requirement to make your research data available to your funder and you must take account of this when recruiting participants.</p> <p>An overview of major funder data policies can be found at the Data Curation Centre - http://www.dcc.ac.uk/resources/policy-and-legal/funders-data-policies</p>		
4.	Does this research entail collaboration with researchers from other institutions and/or across other University Schools/Units?	NO
	<p>If YES state the name(s) and institutions of collaborators:</p>	
5.	If the research is collaborative has a framework been devised to ensure that all collaborators, including all University Staff/Students and External Researchers are given appropriate recognition in any outputs?	NOT APPLICABLE
6.	Where projects raise ethical considerations to do with roles in research, intellectual property, publication strategies/authorship, responsibilities to funders, research with policy or other implications etc., have you taken appropriate steps to address these issues?	NO
7.	Are you using only library; internet sources; unpublished data (<i>with appropriate licenses and permissions</i>) or data in the public domain and so have no human involvement such as interviewing of people? If YES , but the project has other ethical considerations, you should give details of these in Q31; alternatively if there are no ethical considerations sign page 1 and page 6 and submit the form for review.	NO

RESEARCH INFORMATION	
8. a. Who are your participants? (e.g. students aged 18-21)	Individuals aged 35-49 who live or commute to Milton Keynes, are smartphone users, and cycle for pleasure or commute. The number of female and male participants should be equal.
b. How will you recruit your participants?	Participants will be recruited by Qualitative Research Services (QRS), a market research firm based in the South of England. QRS has been used several times by my supervisors to recruit for focus group studies.
c. Estimated duration of participant involvement.	A maximum of one hour.

ETHICAL CHECKLIST If you answer 'NO' to any of questions 12-20 please provide a full explanation in Q31	
9. a. Location of the research	The Open University – Milton Keynes
b. Have you obtained permission to access the site of research	YES
If YES please state agency/authority etc. & provide documentation. If NO please indicate why in Q31	The Open University (Documentation is attached to the application)
10. Will inducement, other than expenses, be offered to participants? If YES, please give details and justification for inducement in Q31	YES
11. Has ethical approval been sought and obtained from any external body eg. REC (NHS)/LEA and or including other UK Universities? If YES, please attach a copy of the external application and approval.	NOT APPLICABLE
12. Will you tell participants that their participation is voluntary?	YES
13. Will you describe the main project/experimental procedures to participants in advance so that they can make an informed decision about whether or not to participate?	YES

14. Will you tell participants that they may withdraw from the research at any time and for any reason, without having to give an explanation?	YES
15. Will you obtain appropriate consent from participants? eg. Oral, written, online tick box – please explain in Q31	YES
16. Please answer either a. or b. a. If the research is photographed or videoed or taped or observational, will you ask participants for their consent to being photographed, videoed, taped or observed?	YES
b. Will participants be free to reject the use of intrusive research methods such as audio-visual recorders and photography?	NOT APPLICABLE
17. Will you tell participants that their data will be treated with full confidentiality and that if published, it will not be identifiable as theirs?	YES
18. Will you tell participants their work /contribution will be credited unless they specifically request anonymity?	YES
19. Will participants be clearly informed of how the data will be stored, who will have access to it, and when the data will be destroyed?	YES
20. Will you give participants a brief explanation in writing of the study after participant involvement explaining where participants can find out about the results of the project and access sources of support, if appropriate?	YES
21. With questionnaires and/or interviews, will you give participants the option of omitting questions they do not want to answer?	YES

WORKING WITH CHILDREN AND/OR VULNERABLE PEOPLE

22. a. Do participants fall into any of the following groups?	
○ Children (under the age of 16 in Scotland or 18 in England and Wales)	<input type="checkbox"/>
○ Protected adult, receiving care or welfare services	<input type="checkbox"/>
○ People with learning or communication difficulties	<input type="checkbox"/>
○ Residents/Carers in a specific location eg. Care Home	<input type="checkbox"/>

○ NHS patients or staff	<input type="checkbox"/>
○ People in custody	<input type="checkbox"/>
○ People engaged in illegal activities (eg. drug taking)	<input type="checkbox"/>

ETHICAL RISK

<p>23. a. Is there any significant risk (inc. physical/psychological harm or distress) to any participants, field assistants, students, collaborators involved in the project?</p> <p>If YES, please provide details of how you intend to mitigate these risks in Q31.</p>	NO
<p>24. a. Have you submitted a fieldwork risk assessment for review and approval, if appropriate?</p>	NO
<p>b. Have you confirmed you are covered by the University travel insurance where the level of risk is deemed to be 'high'? (ie. FCO guidance advises against all but essential travel?)</p>	NO
<p>25. Will your project involve deliberately misleading participants in any way?</p>	NO
<p>26. Are any of the participants in a dependent relationship with the investigator?</p>	NO

CLINICAL RESEARCH / TRIALS

<p>27. a. Does the research involve staff or students using clinical expertise to study human health / wellbeing or human physiological / psychological illness? <i>[ADMIN USE: If 'yes', this is either CR or a CT]</i></p> <p>If NO, proceed to Q28</p>	NO
<p>b. Does the research have to comply with any statutory clinical trial requirements or guidelines in the country in which the trial occurs?</p> <p>NOTE: If outwith the UK, please apply this question in context of the statutory framework of each country in which the trial is being carried out and regulated. <i>[ADMIN USE: If 'yes', this is a CT]</i></p>	Click to select

<p>c. Is cover for non-negligent harm required, as well as legal liability cover?</p> <p><i>[ADMIN USE: If 'yes', this is a CT]</i></p>	<p>Click to select</p>
<p>d. Where you responded 'Yes' to 27 a, b, or c, please tick 'yes' to confirm that you have read and understood the University Insurance briefing papers on CR and CT insurance, including relevant exclusions and geographical restrictions. Please also complete Appendix 1 of this form.</p> <p><i>Briefing papers are available at</i> https://moody.st-andrews.ac.uk/moodle/course/view.php?id=4318</p>	<p>Click to select</p>

DATA MANAGEMENT

Your collection, storage and destruction of personal data should be undertaken in accordance with the following:

- Guidance on transfer/storage/destruction of personal data (available on the UTREC web page)
- Guidance on research participants' data protection rights (available on the UTREC web page)
- The University [FAQ on GDPR](#)
- relevant University policies, referring to relevant guidance where provided: the [University Research Data Management Policy](#) and [Research Data Management](#) web site; the data protection principles as outlined in the [University's Data Protection policy](#); the University's [Information Classification Policy](#); and good research practice as outlined in the University's '[Principles of Good Research Conduct](#)'

In this section, the following definitions are used:

- **Personal data** is information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. **Anonymised data**, meaning data that cannot be linked to an individual using any reasonable means, is NOT personal data. For the purposes of this ethical review application form, the data on **consent forms** should not be considered personal data, although copies of those forms must be securely retained for the lifetime of the research.
- **Special category data** is personal data relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation
- **Fully identifiable data** is personal data that can be directly linked to an individual
- **Pseudonymised data** is personal data that can be indirectly linked to an individual using a 'key'

Examples of information to replace the square brackets in Q30 below: PERSON, e.g. John Doe and Professor X or me and my supervisor/co-researcher(s); SECURE LOCATION, e.g. encrypted USB stick, encrypted and backed-up hard drive, locked filing cabinet, restricted access room; TIME PERIOD, e.g. ('up to' or 'within' can be added) 2 weeks, 1 month, 5 years; EVENT, e.g. the interview, the experiment, the end of the study.

For advice or guidance: on data protection, contact dataprot@st-andrews.ac.uk ; on research data management, contact research-data@st-andrews.ac.uk

<p>28. Will your research entail the collection of personal data?</p> <p>i.e. will any data conform to the definition of personal data at the point at which it will be collected?</p> <p>Please note that for the purposes of this ethical review application form, the data on consent forms should not be considered personal data, although copies of those forms must be securely retained for the lifetime of the research.</p>	<p>YES</p>
<p>29. Will your research entail the collection of special category data?</p>	<p>NO</p>
<p>30. Data Lifecycle</p> <p>This question relates to the approach you will take to ensure the confidentiality of personal data over its full lifecycle (i.e. from collection through to destruction).</p>	
<p>a. Collection and Transfer</p> <p>State what data you will be collecting, whether it will be anonymized, pseudonymised or fully identifiable, briefly indicating how/when you will collect it, and how you will ensure its safe transfer into storage.</p> <p>Data collected will be qualitative and non-attributable. However, to enable participants to register in the focus group, some personal data will inevitably be collected, such as name, surname, and city of residence. These data, however, will be kept separate from any data pertaining to the focus group discussion, and destroyed immediately after the focus group takes place. Furthermore, data will be collected via three voice recorders (one main, and two as back-up) directly recording into a fully encrypted and backed-up external hard-drive accessible to me, my supervisors, and a third-party agency in charge of transcribing the data from the focus groups as per a template I have devised.</p>	
<p>b. Storage, Backup and Access</p> <p>If you are collecting a single form of data, you should indicate the type by selecting ONE checkbox from the three options below and edit the text fields indicated in red capitals to match the particulars of your own research protocol.</p> <p>If you are collecting multiple forms of data, you can select MORE THAN ONE checkbox below and edit the text fields indicated in red capitals to match your own research protocol for</p>	

your respective data types. If you have selected more than one checkbox, you must clearly indicate in **Q31** which data type pertains to which aspect of your research.

Select as appropriate.

<ul style="list-style-type: none"> The data will be stored in an ANONYMISED form, which means that parts of the data will be edited or deleted such that no-one, including the researchers, could use any reasonably available means to identify participants from the data. The un-anonymised data will then be permanently deleted. The anonymised data will be stored in an encrypted and backed-up external hard drive, and only the researcher, supervisors, and a third-party company in charge of transcribing the focus group data will be able to access it. 	<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> The data will be stored in a PSEUDONYMISED form, which means that the data will be edited so that participants are referred to by a unique reference such as a code number or different name, and their original data will be [deleted / remain accessible only to PERSONS]. The pseudonymised data will be stored in [SECURE LOCATION], and only [PERSONS] will be able to access it. There will be a 'key' document, which will link participants' unique reference to their real identity. The key will be kept in [SECURE LOCATION BUT DIFFERENT TO LOCATION OF DATA], and only [PERSONS] will have access to it and be able to reconnect participants' data to them at a later date. 	<input type="checkbox"/>
<ul style="list-style-type: none"> The data will be stored in a FULLY IDENTIFIABLE form, which means that the data will be identifiable as that of the participant. The fully identifiable data will be stored in [SECURE LOCATION], and only [PERSONS] will be able to access it. 	<input type="checkbox"/>

c. Sharing

If you are collecting a **single form of data**, you should indicate the type by selecting **ONE** checkbox from the three options below and edit the text fields indicated in red capitals to match the particulars of your own research protocol.

If you are collecting **multiple forms of data**, you can select **MORE THAN ONE** checkbox below and edit the text fields indicated in red capitals to match your own research protocol for your respective data types. If you have selected more than one checkbox, you must clearly indicate in **Q31** which data type pertains to which aspect of your research.

Select as appropriate.

<ul style="list-style-type: none"> Participants' data will be shared (published and/or placed in a database accessible by others) in an ANONYMISED form, which 	<input checked="" type="checkbox"/>
--	-------------------------------------

means that no-one could use any reasonably available means to identify participants from the data.	
<ul style="list-style-type: none"> Participants' data will be shared (published and/or placed in a database accessible by others) in a PSEUDONYMISED form, which means that participants' data will be edited so that they are referred to by a unique reference such as a code number or different name. There will be a 'key' document, which will link participants' unique reference to their real identity. The key will be kept in [SECURE LOCATION BUT DIFFERENT TO LOCATION OF DATA], and only [PERSONS] will have access to it and be able to reconnect participants' data to them at a later date. 	<input type="checkbox"/>
<ul style="list-style-type: none"> Participants' data will be shared (published and/or placed in a database accessible by others) in a FULLY IDENTIFIABLE form, which means that the data will be identifiable as that of the participant and attributed to them. 	<input type="checkbox"/>

d. Destruction

If you are collecting a **single form of data**, you should indicate the type by selecting **ONE** checkbox from the three options below and edit the text fields indicated in red capitals to match the particulars of your own research protocol.

If you are collecting **multiple forms of data**, you can select **MORE THAN ONE** checkbox below and edit the text fields indicated in red capitals to match your own research protocol for your respective data types. If you have selected more than one checkbox, you must clearly indicate in **Q31** which data type pertains to which aspect of your research.

Select as appropriate.

<ul style="list-style-type: none"> Participants' data will be shared as described above, and then the data held by the researcher will be destroyed 3 years following the end of the project. 	<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> Participants' data will be shared as described above, and then the data held by the researcher will be converted into an anonymous format [TIME PERIOD] following [EVENT] and kept indefinitely in accordance with the safeguards detailed by law, and the un-anonymised data will be destroyed. 	<input type="checkbox"/>
<ul style="list-style-type: none"> Participants' data will be shared as described above, and then the data held by the researcher will be kept indefinitely in accordance with the safeguards detailed by law. 	<input type="checkbox"/>

ETHICAL ISSUES

Several ethical issues are raised by this project. The scenarios employed in the different focus groups ask the participants to make a decision: to donate or not personal data. However, this particular task may be sensitive to some participants as the scenarios portrayed could prove quite personal to some of them, especially if they had their personal data misused in the past. Therefore, in order to address this specific issue, all the scenarios and questions asked are about a fictional character in a fictitious smart city project. This way, instead of diving into details of their personal lives, participants will be discussing what should the character do and the reasoning behind that decision.

Another ethical issue that may arise is if and when the participants share personal details during the discussion. For example, “My mom always said, X you need to think before opening your mouth”, or “Where I live, by the stadium on X street, there are a lot of bikes passing every day”. In this case, the participants will be advised not to disclose any personal information during the conversation, however, if this happens, the transcription company will be instructed to change the personal details with a “P”, to be understood as a reference to their personal information. If the information disclosed does not relate to the participant’s name, the transcription company will enter a “=” before and after the sensitive data.

Acquiring informed consent is also vital for this, and any other, research. Therefore, participants will be provided with accurate information about this project and will also have the opportunity to contact me or my supervisors with any questions they may have. Nonetheless, questions may also be asked orally before the focus groups begin. All the necessary forms will be collected signed before the start of the session. Consent will be asked by asking the participants to sign the relevant form before the start of the focus group. Participants will never be coerced to sign and are free to refuse to participate and leave at any point they wish to.

Furthermore, it is essential to assure the participants that data pertaining to their participation is anonymised and safe from access by unauthorised third-parties. Therefore, the only personal data collected will be the participant's name and surname, that allows them to sign in to the focus group, and, inevitably, city of residence. These

data, however, will be kept separate from any data pertaining to the focus group discussion (data that will be transcribe and analysed), and destroyed immediately after the focus group takes place. The audio recordings will be kept securely and stored separately to any identifiable information (e.g. consent forms). Audio recordings will be taken on an encrypted device, and two back-up encrypted devices, and transcribed at the earliest opportunity before being archived for future use.

Moreover, in order to ensure that this research is inclusive, the physical spaces at the location where the fieldwork takes place (The Open University), are accessible by disabled people, and adjustments will be made to participants who may require them. The participants will be recruited through a market research company named ‘Qualitative Research Services (QRS)’. The researcher has taken note of the committee concerns regarding the offer of incentives and the negative consequences thenceforth. However, the researcher feels that offering an incentive to the participants is a mark of gratitude and respect for their time and willingness to participate. It may also help the participants with any expense they may incur while traveling to the venue. Anything else would be perceived as exploitative by both the participants and the recruiter.

Nonetheless, and in agreement with the committee, the researcher acknowledges the problems that our ‘consumption society’ is unleashing on the planet and its inhabitants. Therefore, and in light of this, the researcher will offer a £30 ‘Cyclechoice’ Gift Card to each participant. This is an alternative incentive that promotes environmentally friendly behaviours among a set of participants who already recognise the benefits related with cycling (Further argumentation is included in the e-mail response).

Besides the issues explored above, no further ethical issues are expected.

Details about the methodology are attached to this application.

DECLARATIONS	
You must not submit your ethical application without first discussing your application with your Supervisor and obtaining their signature. If you submit your application without your Supervisor’s signature, it will be returned to you and this will impact on the timely review of your application.	
<input type="radio"/> I have discussed my research proposal and the ethical implications posed by it with my Supervisor.	<input checked="" type="checkbox"/>

<input type="radio"/> I have read and understood the policies and guidance indicated in the header of the Data Management section and understand my responsibilities as a researcher detailed therein, including those related to data protection.		<input checked="" type="checkbox"/>	
<input type="radio"/> I have read the UTREC guidelines and agree to proceed in line with University ethical guidance.		<input checked="" type="checkbox"/>	
<input type="radio"/> I am aware of the conditions of the funding that I may be in receipt of and will ensure that information given to my research participants is in line with those conditions.		<input checked="" type="checkbox"/>	
<input type="radio"/> I have read and understood the professional guidelines relevant to my specific discipline (eg. BPS, MRC, ASA)		<input checked="" type="checkbox"/>	
Researcher signature		Date	06/06/2019
Supervisor Comment			
I confirm that I have read this application and I approve its submission to the ethics committee for consideration			
Supervisor signature		Date	06/06/2019

APPENDIX 7 – CONSENT FORM



University of
St Andrews

Consent Form

Risk Perceptions in the Donation of Mobility Data
Jorge Campos

The University of St Andrews attaches high priority to the ethical conduct of research. We therefore ask you to consider the following points before signing this form. Your signature confirms that you are willing to participate in this study, however, signing this form does not commit you to anything you do not wish to do and you are free to withdraw your participation at any time.

Please initial box

- ☐ I understand the contents of the Participant Information Sheet (marked '[PIS_[20/05/2019]_[V1]_[Risk Perceptions in the Donation of Mobility Data]') ☐
- ☐ I have been given the opportunity to ask questions about the study and have had them answered satisfactorily. ☐
- ☐ I understand that my participation is entirely voluntary and that I can withdraw from the study at any time without giving an explanation ☐
- ☐ I understand who will have access to my data, how it will be stored, in what form it will be shared, and what will happen to it at the end of the study. I understand that I will be able to withdraw my data within 1 month of the study taking place, and that if my data has been anonymised, it cannot be withdrawn after that point. ☐
- ☐ I agree to take part in the above study ☐

Audio recordings

I understand that part of this research involves taking audio recordings. These recordings will be kept securely and stored separately to any identifiable information, i.e. consent forms and questionnaires. Audio data can be a valuable resource for future studies and, therefore, we ask for your additional consent to maintain this data for this purpose.

- ☐ I agree to being audio recorded ☐
- ☐ I agree to my audio material to be published as part of this research. ☐

- I give permission for my audio material to be used in future studies without further consultation.



Signatures			
I confirm that I am willing to take part in this research			
	Print name	Date	Signature
Participant			
Researcher	Jorge Campos	20/05/2019	

APPENDIX 8 – PARTICIPANT INFORMATION SHEET



University of
St Andrews

Participant Information Sheet

Risk Perceptions in the Donation of Mobility Data
Jorge Campos

What is the study about?

We invite you to participate in a research project which aims to understand the different risks perceived by individuals when deciding whether to donate their personal mobility data to a smart city project.

Do I have to take part?

This information sheet has been written to help you decide if you would like to take part. It is up to you and you alone whether you wish to take part. If you do decide to take part you will be free to withdraw at any time without providing a reason.

What would I be required to do?

You have been invited to participate in a focus group that has a maximum duration of one hour. In the focus group, you will be asked to discuss different scenarios with other members of the group and with the facilitator. These scenarios will feature a fictitious person deciding whether or not to donate their mobility data.

Are there any risks associated with taking part?

There are no foreseeable risks associated with taking part in this project.

Informed consent

It is important that you are able to give your informed consent before taking part in my project and you will have the opportunity to ask any questions in relation to the research before you provide your consent. You may ask these questions by writing (you may find my e-mail contact at the bottom of this form), or orally before the focus group starts. If you are satisfied, and still wish to take part, you will be asked to sign a consent form on the day the focus group takes place.

Who is funding the research?

The research is being funded by the University of St Andrews.

Reward

As a thank you for your time and willingness to participate, we will provide you with a £30 'Cyclechoice' Gift Card when the focus group is completed.

What information about me or recordings of me ('my data') will you be collecting?

The personal data we collect will be limited to name, surname and city of residence to enable you to sign in to the focus group session. These personal data will be destroyed the day after the focus groups takes place. All audio recorded data collected in the focus group will be anonymised before being analysed. The audio recordings will be kept securely and stored separately to any identifiable information (i.e. consent forms, debrief).

How will my data be stored, who will have access to it?

Your data will be stored in an **ANONYMISED** form, which means that parts of your data will be edited or deleted such that no-one, including the researchers, could use any reasonably available means to identify you from the data. Your un-anonymised data will then be permanently deleted. Your data will be stored in an encrypted, password-protected and backed-up external hard drive, and only the researcher and supervisors will have access to it. Additionally, a trusted third-party company in charge of the transcription of the audio data will be able to access the recordings in order to transcribe them. However, this third party-company will not have access to any of the forms that contain your personal data.

Audio recordings will be taken on an encrypted device and transcribed at the earliest opportunity before being archived for future use. Furthermore, the devices used in the recording, processing, and storing of data, are encrypted and password protected.

How will my data be used, and in what form will it be shared further?

Your research data will be analysed as part of the research study, and may be published and used for future scholarly research without further consultation. Your data will be shared (published and/or placed in a database accessible by others) in an **ANONYMISED** form, which means that no-one could use any reasonably available means to identify you from the data.

It is expected that the project to which this research relates will be finalised by July of 2020 and written up as part of my PhD thesis.

When will my data be destroyed?

Your data will be shared as described above, and then the data held by the researcher will be destroyed 3 YEARS following the conclusion of this project.

International data transfers – Personal data

Your data will be stored and processed in an encrypted and backed-up external hard drive. No matter their physical location, researchers are required to store and make

use of personal data as if they were in the UK; University requirements and the provisions of the data protection law apply at all times.

Will my participation be confidential?

Yes, your participation will only be known to the researcher and supervisors. Additionally, a trusted third-party company in charge of the transcription of the audio data will be able to access the recordings in order to transcribe them. However, this third party-company will not have access to any of the forms that contain your personal data.

Lawful basis for making use of personal data and data protection rights

The lawful basis that the University will rely on to make use of your personal data during the research and for related research projects in the future, as described to you is public task; where special category personal data are used the lawful basis is archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The University of St Andrews is a Data Controller for the information you provide about you. You have a range of rights under the data protection legislation, including the right of complaint. However, some of those rights may not be available where you provide personal data for research purposes. For questions, comments or requests, consult the University website at <https://www.st-andrews.ac.uk/terms/data-protection/rights/>, or email dataprot@st-andrews.ac.uk.

You will be able to withdraw your data within 1 month. If your data is anonymised, we will not be able to withdraw it after that point, because we will no longer know which data is yours.

Ethical Approvals

This research proposal has been scrutinised and subsequently granted ethical approval by the University of St Andrews Teaching and Research Ethics Committee.

What should I do if I have concerns about this study?

In the first instance you are encouraged to raise your concerns with the researcher and if you do not feel comfortable doing so, then you should contact my Supervisor. A full outline of the procedures governed by the University Teaching and Research Ethics Committee is available at www.st-andrews.ac.uk/utrec/guidelinespolicies/complaints/

Contact details

Researcher(s) Jorge Campos

jfpc@st-andrews.ac.uk

Supervisor(s) Kirstie Ball / Sally Dibb

Kirstie.Ball@st-andrews.ac.uk

APPENDIX 9 – DEBRIEFING SHEET



University of
St Andrews

Debrief

Risk Perceptions in the Donation of Mobility Data
Jorge Campos

Thank you for taking part in my research project; your contribution is valuable.

Nature of study

This project aims to understand how individuals perceive privacy risks when deciding whether to donate their personal mobility data to a smart-city project. In order to explore this phenomenon, it is necessary to conduct scenario-based focus groups so that patterns of risk can be elicited, and, later, identified.

Data

As outlined in the Participant Information Sheet (marked: 'PIS_[20/05/2019]_[V1]_[Risk Perceptions in the Donation of Mobility Data]');

- The information (data) you have provided will be stored in an anonymised form.
- Your information (data) will be stored in an encrypted and backed-up external hard drive and only the researcher, supervisors, and a trusted third-party company in charge of the transcription will be able to access it.
- Your data will be shared (published and/or placed in a database accessible by others) in an anonymised form.

- Your information (data) will be shared as described above, and then the information (data) held by the researcher will be destroyed 3 years following the conclusion of this study.]
- If you no longer wish to participate in the research, you are free to withdraw at any time. You will be able to withdraw your data within 1 month. If your information (data) is anonymous at the point of collection or subsequently anonymised, we will not be able to withdraw it after that point because we will no longer know which information (data) is yours.

Contact

If you have concerns or if you would like to view a summary of the results of my research, please email the researcher or the supervisor detailed below.

Researcher(s) Jorge Campos

jfpc@st-andrews.ac.uk

Supervisor(s) Kirstie Ball / Sally Dobb

Kirstie.Ball@st-andrews.ac.uk

APPENDIX 10 – ETHICAL AMENDMENT FORM

University of St Andrews

Teaching and Research Ethics committee (utrec)

ETHICAL AMENDMENT FORM

Please Tick: (click on the box then click 'Checked' for a cross to appear in the box)

Undergraduate ☐ Postgraduate Research ☒ Postgraduate Taught ☐ Staff ☐

Lecturer/Course Controller on behalf of Taught module ☐ Module Code:

(Please do not type out with text boxes provided, note that the Text Boxes are fixed in size and will not allow any viewing beyond the word limit permitted.)

Researcher Name(s):	Jorge Pereira Campos		
Original Title:	Risk Perceptions in the Donation of Mobility Data		
Supervisor :	Kirstie Ball	Email(s):	jfpc@st-andrews.ac.uk Ksb9@st-andrews.ac.uk
Approval Code:	MN14450		

Amended Title: (if applicable)			
Additional Researchers (if applicable)			
School/Unit: (Please indicate)		Submission Date:	

Amended Rationale: Please give a BRIEF description of the amendments made to your project, including reasoning for, in 'lay language'. (NOTE; where substantial amendments, in rationale or ethical considerations are to be made please fill in a complete new Ethical Application Form rather than this amendment form). *This summary will be reviewed by UTREC and may be published as part of the reporting procedures. DO NOT exceed 75 Words (for database reasons).*

Incentive amount has been increased to £40 and will be given in cash rather than as a voucher.

Amended Ethical Considerations: Please indicate any 'new' ethical considerations brought about by the amendment of your project. *This summary will be reviewed by UTREC and may be published as part of the reporting procedures. DO NOT exceed 75 Words (for database reasons).*

Risk to researcher.

The researcher will have to travel to the research venue and his overnight accommodation with a large amount of cash on his person which presents a risk. A number of mitigating actions will need to be undertaken (see next section)

ETHICAL STATEMENT

Write a clear but concise statement of the ethical considerations raised by the project and how you intend to deal with them. It may be that in order to do this you need to expand on the Ethical Considerations section on page 1. (continue on additional pages if necessary)

Relating to the INCENTIVE AMENDMENT

The researcher will have to travel to the research venue and nearby accommodation carrying cash rather than voucher incentives. The following risk mitigation actions have been undertaken.

Cash will be carried by the researcher in a sealed envelope contained in a bag and will not leave the researcher's person at any time on the way to the research venue.

Cash will be stored in a safe at the accommodation near to the research venue (Hilton Hotel Milton Keynes)

Cash will only be removed from the safe when it is required for a particular focus group. Thence it will be decanted into individual envelopes, each addressed to a specific participant

Upon receipt of the cash, the participant will sign and date a signature sheet indicating that they have received the cash.

This signature sheet will be presented to Accounts Payable after the fieldwork to indicate how the cash has been spent. In the event of a no – show, monies will be paid back to the University.

DOCUMENTATION CHECKLIST

Ethical Amendment Application Form	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Amended Participant Information Sheet	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Amended Consent Form	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Amended Debriefing Form	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Amended Questionnaire	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Amended Advertisement	YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
Other (please list):	<div></div>			

DECLARATION

I am familiar with the UTREC Guidelines for Ethical Research <http://www.st-andrews.ac.uk/utrec/guidelines/> and *BPS, *ESRC, *MRC and *ASA (*please delete the guidelines not appropriate to your discipline) Guidelines for Research practices, and have discussed them with other researchers involved in the project.

STAFF

YES ☐ NO ☐

Print Name:

Signature

Date:

STUDENTS ONLY

My Supervisor has seen and agreed all relevant paperwork linked to this project

YES ☒ NO ☐

Print
Name:

JORGE FERNANDO PEREIRA CAMPOS

Signat
ure

Date:

04.09.201

SUPERVISOR(S)

The Supervisor must ensure they have read both the application and the guidelines, and also has approved the project and application, before signing below, with clear regard for the balance between risk and the value of the research to the School/Student

Print Name:		
Signat ure		
Date:		